ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

ANÁLISIS DE ALGORITMOS CRIPTOGRÁFICOS CLÁSICOS VS ALGORITMOS CUÁNTICOS

CARMEN ELENA MANTILLA CABRERA

Proyecto de investigación, presentado ante el Instituto de Posgrado y Educación Continua de la ESPOCH, como requisito parcial para la obtención del grado de

MAGISTER EN SEGURIDAD TELEMÁTICA

RIOBAMBA-ECUADOR

Enero 2018

ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

CERTIFICACIÓN:

El tribunal del PROYECTO DE INVESTIGACIÓN CERTIFICA QUE:

El proyecto de investigación titulado "ANÁLISIS DE ALGORITMOS CRIPTOGRÁFICOS CLÁSICOS VS ALGORITMOS CUÁNTICOS", de responsabilidad de la Ing. Carmen Elena Mantilla Cabrera ha sido prolijamente y se autoriza su presentación.

Tribunal:

Dr. Juan Mario Vargas Guambo, M.Sc. **PRESIDENTE**	**FIRMA**
Ing. Ruth Genoveva Barba Vera, Mg. **DIRECTOR**	**FIRMA**
Ing. José Enrique Guerra Salazar, Mg. **MIEMBRO DEL TRIBUNAL**	**FIRMA**
Dr. José Rigoberto Muñoz Cargua, M.sC. **MIEMBRO DEL TRIBUNAL**	**FIRMA**

Riobamba, Enero 2018

DERECHOS INTELECTUALES

Yo, Carmen Elena Mantilla Cabrera, con cédula de identidad 060298013-8 soy responsable de las ideas, doctrinas, resultados y propuestas expuestas en la presente investigación y los derechos de autoría pertenecen a la Escuela Superior Politécnica de Chimborazo.

Carmen E. Mantilla C.

C.I.: 0602980138

DECLARACIÓN DE AUTENTICIDAD

Yo, Carmen Elena Mantilla Cabrera, declaro que el presente Proyecto de Investigación, es de mi autoría y que los resultados del mismo son auténticos y originales. Los textos constantes en el documento que provienen de otra fuente están debidamente citados y referenciados.

Como autor/a, asumo la responsabilidad legal y académica de los contenidos de este proyecto de investigación de maestría.

Riobamba, 2018

_____

Carmen E. Mantilla C.

C.I.: 0602980138

DEDICATORIA

Dedico este trabajo esta tesis en especial a mis hijos que han sacrificado horas a su lado para culminar esta meta y a mi familia que me ha brindado apoyado incondicional en cada uno de mis proyectos de vida, no solo moralmente si no con acciones para que pueda culminar estos desafíos.

Carmen E. Mantilla C.

AGRADECIMIENTO

A mis tutores por haber guiado este trabajo de titulación con sus conocimientos en la elaboración de la investigación.

A todas aquellas personas que han intervenido de alguna u otra forma en el proceso de realización de esta tesis para que culminar con éxitos, mi infinito agradecimiento

Carmen E. Mantilla C.

ÍNDICE DE CONTENIDOS

INDICE DE TABLAS

INDICE DE GRÁFICOS

ÍNDICE DE ANEXOS

RESUMEN

En este trabajo de investigación se realizó una comparación de los algoritmos criptográficos cuánticos vs clásicos con respecto a la seguridad en la obtención de la clave, en base a una revisión sistemática de donde se definió parámetros medibles de comparación, entre estos algoritmos como: la unidad estructural de la información, base de su seguridad, origen de la clave, tamaño de la clave, si el atacante copia la información, detección de intrusos y tecnología aplicada en el mercado, es de importancia conocer el algoritmo criptográfico más fuerte para la seguridad de la información debido a que la tecnología va en incremento y al mismo tiempo la información se convierte en un activo de gran valor a proteger ya que los hackers al interceptar información pueden realizar denegación de servicios, falta de integridad en datos, daños físicos a estructuras, robos millonarios de dólares e información. También se desarrolló el estudio técnico-económico para la de implementar un sistema cuántico en una infraestructura gubernamental del Consejo Nacional Electoral (CNE). Del estudio se determinó que los algoritmos criptográficos cuánticos son más apropiados para este propósito, esto se demostró con el método estadístico CHI cuadrado, para la comprobación de hipótesis. Se concluye que es técnicamente factible la propuesta de implementar criptografía cuántica con el algoritmo BB84 en la estructura nacional gubernamental CNE, con una inversión aproximada al 0.022% del gasto público de 2017. Se recomienda implementar la propuesta técnica económica planteada en la presente investigación para en la infraestructura de CNE en función de garantizar la seguridad de la información.

Palabras clave: <TECNOLOGÍA Y CIENCIAS DE LA INGENIERÍA>, <SEGURIDAD TELEMÁTICA>, <CRIPTOGRAFÍA CUANTICA>, <CRIPTOGRAFÍA CLÁSICA>, <ALGORITMOS CRIPTOGRÁFICOS>, <IMPLEMENTACIÓN DEL SISTEMA CUANTICO>

SUMMARY

In this research work, a comparison of quantum vs classical cryptographic algorithms was made with regard to the security in obtaining the key, it was based on a systematic review where measurable parameters of comparison were defined, among these algorithms as: the structural unit of information, base of its security, key origin, key size, if the attacker copies the information, intrusion detection and technology applied in the market, it is important to know the strongest cryptographic algorithm for the security of the information because the technology is increasing and at the same time the information becomes a valuable asset to protect since the hackers when intercepting information can perform denial of services, lack of data integrity, physical damage to structures, thefts of millions of dollars and information. Also the technical-economic study was developed to implement a quantum system in a governmental infrastructure of the National Electoral Council (NEC). From the study, it was determined that the quantum cryptographic algorithms are more appropriate for this purpose; this was demonstrated with the CHI square statistical method, for the verification of the hypothesis. It is concluded that the proposal to implement quantum cryptography with the BB84 algorithm in the national government structure NEC is technically feasible, with an approximate investment of 0.022% of public expenditure in 2017. It is recommended to implement the economic technical proposal raised in this research for the infrastructure of NEC in order to guarantee the security of the information.

Keywords: < TECHNOLOGY AND ENGINEERING SCIENCE >, <TELEMATIC SECURITY>, <QUANTUM CRYPTOGRAPHY>, <CLASSIC CRYPTOGRAPHY>, <CRYPTOGRAPHIC ALGORITHMS>, <IMPLEMENTATION OF THE QUANTUM SYSTEM >,

CAPÍTULO I

1. INTRODUCCIÓN

Los avances tecnológicos especialmente en las comunicaciones dan pasos gigantescos ayudando al desarrollo económico y social de los países. Las telecomunicaciones son tan necesarias en la vida cotidiana para comunicarnos con familiares, difundir información, ventas, banca, entretenimiento, organismos gubernamentales, etc., es evidente la influencia de la tecnología y su crecimiento inexorablemente facilitado tanto nuestras vidas de forma que cualquier empleado de una empresa puede trabajar desde su casa, estar disponible en cualquier momento y sitio, esto da lugar a la existencia virtual, pero la inconsciencia de usuarios de las tecnologías es alarmante, una cultura de malas prácticas de seguridad informática, rompiendo las reglas de privacidad y anonimato creando escenarios vulnerables a ataques cibernéticos (Mogos., 2016).

Es común escuchar en los noticieros los ciberataques se incrementan, roban datos de cuentas, nicks de personajes públicos hackeadas, Anonymous ataca otra vez, ciberataques una nueva guerra fría. Pero que hay detrás de estos titulares, consecuencias como las de Estonia en 2007 el ataque a todo un país donde las páginas web de bancos, medios de prensa y organismos gubernamentales colapsaron quedando incomunicados sin estos servicios por semanas generando caos y desconcierto en el país. Una de las consecuencias de los ataques que más daños pudo haber causado fue STUXNET un ataque dirigido a las centrales nucleares Natanz, Irán en 2010, donde se tomó el control de 1000 máquinas a las cuales se reprogramaron para realizar un trabajo acelerado que con el tiempo y por la velocidad se desintegraron, fue el primer ciberataque que logra destruir la infraestructura del mundo real (McGuinness, 2017; Turing, 2013).

Según el informe de ciberseguridad del Banco Internacional de desarrollo, la mayoría de los países de América Latina y el Caribe no tiene la capacidad adecuada para contrarrestar la amenaza del cibercrimen, menciona que de cada cinco países, cuatro no tienen estrategias de ciberseguridad o planes de protección de infraestructura crítica; de cada

tres, dos no cuentan con un centro de comando y control de seguridad cibernética. El costo del cibercrimen para América Latina y el Caribe es de US$90.000 millones al año (BID, 2017).

En Ecuador en 2015 los sistemas gubernamentales como fiscalía, QUIPUX, Ministerio de Salud fueron atacados constantemente por casi quince días consecutivos, impidiendo desarrollar las actividades normalmente en estas instituciones del estado, evitando la disponibilidad de estos servicios y el contenido de las paginas fueron modificados. Inclusive las universidades de Ecuador en el año 2016 fueron blanco de ataques informáticos donde se vulneró la integridad de los datos de los sistemas académico, por un grupo de hackers que cobraban para cambiar notas. Según el Departamento de tecnologías de la Información y Comunicación DTIC-ESPOCH, nuestra Universidad no fue la excepción, se cambiaron notas y el contenido de su portal web, Joomla Jungle aprovechó de la vulnerabilidad Cross File Transfer para este propósito. Esto evidencia que la falta de seguridad puede causar daños materiales, robos bancarios, fraudes y chantajes o hacer uso de información a favor de terceros cometiendo ilícitos, motivo por el que se debe proteger la información sensible (TheHacker, 2017).

Para proteger la información se utiliza criptografía clásica que son algoritmos para la encriptación de claves pseudo aleatorias, algunos de ellos son RSA, Diffie-Hellman, DES, 3DES, cada uno tiene su complejidad debido a las leyes matemáticas que utiliza y su velocidad depende del número de pasos que ejecute. Pero la mente humana junto al avance de la tecnología han desarrollado técnicas para descifrar la información cifrada que viaja por la red, con ello cada vez es menos seguro ya que la potencia de los nuevos computadores podrían descifrar las claves en menos tiempo. Como solución a este problema se ha implementado la criptografía cuántica como seguridad de la transmisión de datos debido a que son teóricamente aleatorias e indescifrables. A nivel mundial los científicos están realizando investigaciones para desarrollo y aplicación de la criptografía cuántica como una alternativa efectiva en la seguridad de la información (Boneh, 1998).

En 1984 se publica el primer protocolo que utiliza los principios de la mecánica cuántica para garantizar la transmisión de la información segura. Una de las propiedades más importantes de la criptografía cuántica es que sí una entidad diferente al emisor y receptor intenta usar técnicas de ataques de escucha secreta para obtener la llave secreta develará su intención antes de ser transmitida la información privada. Cumpliendo el principio de

incertidumbre de Heisenberg el cual reza que el hecho de medir un sistema cuántico lo perturba, las llaves se codifican mediante el uso de partículas de luz llamadas fotones; estos puntos deben compartir una llave aleatoria, técnicamente indescifrable, descartando la posibilidad de interceptación por parte de terceros (Svozil, 2011).

Una de las aplicaciones que dio veracidad de seguridad de la criptografía cuántica fue el proyecto "Swiss Quantum" por encabezado el físico N. Gisin, de uso gubernamental en las elecciones de Ginebra (Suiza) en Octubre 2007 utilizada por primera para asegurar el conteo de votos que conectaba a la central por fibra óptica con el punto general de recepción de votos permitiendo detectar si los datos enviados fueron alterados o afectados por ruidos aleatorios o intencionales durante la transmisión.

Es importante mencionar experimentos llevados a cabo como el de NIST/Laboratorio de Los Álamos en el que se implementó la criptografía cuántica a una distancia de 148 km y el experimento montado por una colaboración europea en 2007 en espacio abierto a una distancia de 144 Km entre dos de las Islas Canarias. Sugiere que la criptografía cuántica podría también utilizarse en el futuro para comunicaciones satelitales y a medida que pasa el tiempo el avance de la tecnología en esta área (Hernández & Reyes, 2014).

En el Instituto Politécnico Nacional, se realizó un análisis y mejora del rendimiento del algoritmo AES para su utilización en teléfonos móviles, compara los algoritmos clásicos simétricos y asimétricos para elegir uno y aplicarlo a teléfonos celulares para cifrar la información. Hace una comparación de las características, ventajas y desventajas de estos, cabe recalcar que el algoritmos aplicado tiene con limitación la capacidad de procesamiento de equipo celular (Gálvez, 2014).

Una investigación doctoral de la Universidad Alicante , realizó una Propuesta y Análisis de Criptosistemas de Clave Pública Basados en Matrices Triangulares Superiores por Bloques, donde presenta un análisis de la estructura matemática de los algoritmos clásicos asimétricos (Frances, 2013).

En la ESPOCH en conjunto con investigadores Prometeo, se desarrolló una simulación computacional de una aplicación informática cliente-servidor integrado técnicas de autenticación y de encriptación cuántica, se realizó una comparación del porcentaje de copia teórico (Mogos, 2015). Y una investigación de master que realizó un análisis de

algoritmos matemáticos de criptografía pública para mejorar el aprendizaje de la materia de criptografía en la carrera de ingeniería en sistemas de la ESPOCH, el autor analizó los algoritmos asimétricos, determinando que el más adecuado para la enseñanza de la criptografía es RSA (Paguay, 2015).

Del estudio realizado se deriva que investigaciones previas no se enfocan en determinar sustentadamente si los algoritmos criptográficos clásicos o cuánticos son más adecuados para la seguridad en la obtención de clave, que no se establecen parámetros de similitudes para que permitan comparaciones y que no se realizan estudios de factibilidad técnica ni económica en el país para la implementación de sistemas criptográficos cuánticos en Ecuador.

Con los antecedentes antes expuestos se determina que es necesario hacer una revisión bibliográfica sistematizada para contestar la pregunta que otras investigaciones aun no plantean la cual es: ¿Los algoritmos cuánticos son más adecuados para la seguridad en la obtención de clave que los algoritmos clásicos? con el objetivo de trazar un punto de partida para las investigaciones sobre este tema, estudio que permita demostrar y destacar las ventaja de los algoritmos cuánticos con respecto a los clásicos.

Este trabajo tiene como objetivo determinar las ventajas de la criptografía cuántica vs la criptografía clásica respecto a la seguridad en la obtención de claves, tomando como base publicaciones científicas especializadas sobre criptografía cuántica, bases de datos de internet, que mediante una revisión sistemática permitió integrar de forma objetiva los desarrollos realizados sobre el tema, determinar los parámetros bajos los que se comparan la seguridad de los algoritmos clásicos vs cuánticos y determinar la factibilidad de la implantación de un sistema criptográfico cuántico en Ecuador.

1.1. Problema de la investigación

En este apartado se presenta la problemática de la investigación.

1.2. Planteamiento del Problema

A diario la tecnología avanza y las personas hacen uso de esta en las actividades diarias como manejo de banca, comunicación telefónica, comunicación por internet, compras en línea, entidades gubernamentales y privados etc., los denominados hackers están interesados interceptan esta información sin que nos demos cuenta para hacer uso ilícito de dicha información.

Con el fin de proteger los datos que se utilizan para realizar actividades cotidianas se utiliza la criptografía para cifrar la información transmitida con claves y al ser interceptada no sea legible. Se dice que la fortaleza de un algoritmo criptográfico es que da seguridad, se debe a varias cualidades que tiene cada algoritmo como la complejidad, estructura matemática, velocidad, entre otros. En la actualidad los algoritmos clásicos se utilizan para aseguramiento en las transmisiones de datos con números pseudo aleatorios que lo hace determinístico. Como una solución más efectiva se presenta al área de las comunicaciones experimentalmente los algoritmos cuánticos, que utiliza las bondades de la física cuántica por este motivo, utiliza números aleatorios brindando mayor seguridad en la transmisión de datos.

Al ser una tecnología nueva la criptografía cuántica no existen estudios que puedan evidenciar la efectividad en la seguridad de la información de los algoritmos cuánticos respecto a los algoritmos clásicos mediante un estudio de su estructura matemática, complejidad, velocidad, ventajas y desventajas. Al realizar un análisis comparativo entre estas dos tecnologías aplicadas en la criptografía se pretende introducir al nuevo mundo de la criptografía cuántica dando un referente a los algoritmos clásicos y por la forma que están constituidos a los ataques que son vulnerables.

Por otra parte las políticas nacionales buscan garantizar la seguridad de la información en las infraestructuras para servicios públicos para una mejor calidad con el uso de las tecnologías, por lo que en el Plan Nacional del Buen Vivir se presentan objetivos hacia este camino.

Este sería un gran aporte ya que Ecuador hace uso de la tecnología para su desarrollo y no se están realizando estudios de este tipo, pero necesita conocer la efectividad de la criptografía para seguridad de la información.

1.2.1. Formulación del Problema

¿Cuál algoritmo criptográfico es el más adecuado para la seguridad en la obtención de claves?

1.2.2. Sistematización del Problema

- ¿Qué tipo de algoritmos criptográficos se aplican para la seguridad en la obtención de claves tanto en los clásicos como en los cuánticos?
- ¿Cuáles son las ventajas y desventajas de los algoritmos estudiados?
- ¿Cómo trabajan estos algoritmos?
- ¿Cuál es el más adecuado para la seguridad en la obtención de clave tanto de los clásicos como de los cuánticos?
- ¿Bajo qué parámetros se los puede comparar?
- ¿Cuál es el más adecuado para la seguridad en la obtención de clave?

1.3. Justificación de la Investigación

Tareas como compras con tarjetas de crédito en supermercados, mensajes y conversaciones en teléfonos celulares, email, chats, llamadas en línea, búsquedas seguras, compras en línea, almacenamiento en la nube desde su computador, teléfonos, tables, banca en línea, comunicación interna en bancos, electricidad, agua, claves de carros, claves de puertas electrónicas, servicios gubernamentales de comunicación interna y en línea, historial médico con médico particular u hospitales, incluso pasar por alto la vigilancia gubernamental y la censura son cotidianas y necesarias pero en todas estas la seguridad juega un papel importante, lo que se soluciona aplicando la criptografía para la seguridad en la obtención de clave.

Al realizar un estudio comparativo de los algoritmos clásicos con los cuánticos se expuso las ventajas de los algoritmos cuánticos en las seguridades de transmisión de datos por lo que tenemos que forzarnos a pensar de manera cuántica y explotar de esa manera todos los beneficios que pueden brindar este tipo de algoritmos. Y lo que aún falta por explorar ya que se está acostumbrado a que lo cotidiano sea clásico.

La carencia de este tipo de estudios en un país en desarrollo como Ecuador y por ende de sistemas fuertes de seguridad para obtención de claves, hace que el interés de los hackers se vuelva a ellos y que sean presa fácil de ataques informáticos, al realizar estudios de esta temática permitió entender cómo funcionan y en un futuro no muy lejano se podría implementar para la seguridad en el país.

1.4. Objetivos

1.4.1. General

Establecer un análisis comparativo de los algoritmos criptográfico clásicos y los algoritmos cuánticos en la seguridad de la obtención de la clave criptográfica.

1.4.2. Específicos

- Realizar un estudio de los algoritmos criptográficos clásicos y cuánticos.
- Estudiar las teorías matemáticas en la que se fundamenta estos algoritmos criptográficos.
- Determinar que algoritmos se van a comparar en los clásicos y los cuánticos respecto a los parámetros definidos.
- Definir los parámetros bajo los cuales se va a realizar el análisis comparativo de los algoritmos de criptografía cuánticos y clásicos.

1.5. Hipótesis

Los algoritmos cuánticos son más adecuados que los algoritmos clásicos para la seguridad en la obtención de clave.

CAPITULO II

2. MARCO DE REFERENCIA

En este capítulo se analizaron conceptos de criptografía tanto clásica como cuántica y los algoritmos que las constituyen, destacando las ventajas y desventajas de cada uno de estas ya que se consideran necesarios para el desarrollo de esta investigación que busca determinar un análisis comparativo entre algoritmos clásicos y cuánticos en la seguridad de obtención de la clave mediante parámetros que van a ser analizados.

2.1. Criptología

Es un término que abarca tanto el concepto de criptografía que se utiliza para que un texto sea legible únicamente para el receptor al que fue dirigido y el concepto de criptoanálisis que son métodos para descifrar el texto cifrado.

Su importancia radica desde tiempos antiguos donde las personas intentaron por diferentes métodos enviar información en forma secreta por medio de mensajeros en caso de que este sea interceptado, la información que estaba llevado sea ilegible para la persona que no fue dirigida, pero de algún modo, el remitente para el que fue enviada esta información pueda entenderla o descifrarla (Galende, 1995). La criptografía se usó en las guerras para enviar información de tácticas y técnicas a usarse en el campo de batalla que ideaban los altos mandos a las tropas, de tal forma que el éxito de una batalla se reduce a interceptar y descifrar los mensajes de los enemigos (Beckman, 2002); Singh, 2000); Churchhouse, 2014); Kahn, 1973).

2.2. Criptosistemas

Es un par de algoritmos que toman una clave en texto claro que es lo que quiere proteger y lo convierten el texto en una cadena cifrada (Caesar, 2013). Los criptosistemas deben cumplir la condición que se presenta en la ecuación 2.1.(Beth, 1992):

$$D * k\big(E * k(m)\big) = m \qquad (2.1)$$

Dónde:

m: mensajes sin cifrar.

k: claves del criptosistema.

E: transformaciones de cifrado o funciones aplicadas a *m* para obtener un elemento cifrado

D: descifrado, análogo a *E*.

Es el sistema donde el mensaje a cifrar tiene igual longitud de caracteres que la clave a usarse y no tienen relación, pero en el lenguaje natural existe la redundancia de información y hay que tomar en cuenta este factor al momento de generar claves, en el lenguaje en español por lo general cuando un mensaje es incompleto se puede deducir la información faltante por medio de la redundancia o repetición de patrones de palabras que el emisor usa para el mensaje. (Donado, Niño, & Flechas, 2001). Los ataques por fuerza bruta asocian un determinado mensaje con el lenguaje natural de las personas, buscando opciones de palabras acertadas, que son realizados por medios informáticos y algoritmos de criptoanálisis (Frances, 2013).

2.2.1. Teoría de Algoritmos

Identifica la solución óptima para resolver un problema y el tiempo que demora en ejecutarse, un algoritmo es un conjunto finito de pasos que permiten la resolución de un problema, las computadoras son capaces de ejecutarlos a velocidades distintas, producen muchas operaciones matemáticas por segundo dependiendo de su CPU. La teoría de algoritmos permite conceptualizar el término de invarianza, que induce a la compresión

de que el tiempo de ejecución de un algoritmo es constante en cualquier computador siempre y cuando el conjunto de datos de entrada del algoritmo sea muy extenso (Gálvez, 2014).

2.3. Cifrados Simétricos

Es un método criptográfico que usa la misma clave para cifrar y descifrar, por lo que al transmitirse la información si se intercepta la clave permite el acceso a la información. Por esta razón los algoritmos de cifrado simétrico presentan desventajas frentes a los de criptografía asimétrica. Algunos de los algoritmos criptográficos simétricos son DES y AES (Daemen & Rijmen, 2001; Thakur & , Kumar, 2011).

2.3.1. Algoritmo AES

AES sus siglas en inglés Advanced Data Encryption Standard, fue publicado en 2001, presenta diferencias notables con respecto al resto de los cifradores simétricos, el tamaño de los bloques de 128 bits, maneja claves de longitudes diferentes y uso de matemáticas polinomiales en estructuras de campos finitos, al procesar datos en bloques de tamaño fijo con claves de diferentes longitudes impacta en el número de iteraciones que van de 10 a 14, no altera la longitud del criptograma, genera de 128 bits que se realizan durante el cifrado/descifrado. (Corrales, Cilleruelo & Cuevas, 2011; Gálvez, 2014).

2.3.2. Algoritmo DES

En 1976 fue adoptado como estándar por el Gobierno de los EE.UU. para comunicaciones no clasificadas, es el más usado a nivel mundial, se basa en el algoritmo LUCIFER, desarrollado por IBM. DES codifica bloques de 64 bits emplea claves de 56 bits. Es una Red de Feistel de 16 rondas, más dos permutaciones, una que se aplica al principio (Pi) y otra que se aplica al final (Pf), donde la segunda es la inversa de la primera (Gálvez, 2014). Es vulnerable a los ataque por fuerza bruta.

2.3.3. Algoritmo IDEA

Es un algoritmo que trabaja con bloques de 64 bits, con clave de 128 bits imposibilita un ataque por la fuerza bruta, es muy seguro, resistente a varios ataques como el criptoanálisis diferencial, se basa en los conceptos de confusión y difusión, hace uso de operaciones elementales: XOR, suma módulo 216, producto módulo 216 +, (Gálvez, 2014).

2.4. Cifrados Asimétricos

A diferencia de los simétricos que tienen dificultad para el intercambio de claves en la comunicación segura entre el transmisor y receptor, facilitan la distribución de claves, entonces los sistemas de cifrados de clave pública funcionan con dos claves, una pública que conocen todos, y una clave privada que es secreta pero conocida solo por una persona (Landa, 2015). Para encriptar la información necesita mayores recursos computacionales que para los de clave simétrica, para solucionar este problema se combina ambos métodos generando el cifrado híbrido. Dentro de los principales algoritmos de claves asimétricas podemos citar los siguientes: RSA, Diffie-Hellman, ElGamal, El Rabin (Corrales., 2011).

2.4.1. Algoritmo RSA

Creado en 1977, creado por Ron Rivest, Adi Shamir y Leonard Adleman, el algoritmo RSA radica su fortaleza en cálculos y factorización de números primos para generar claves públicas y privadas. Determina la inversa de la factorización mediante la operación modular de números grandes imposible actualmente romper este cifrado, la relación de encriptar y desencriptar es simple. Un mensaje solo puede ser visto por el receptor que posee la clave pues estas no se pueden deducir de otras (Benet, 2015; Saudi, 1998). En la tabla 1-2 se muestra un resumen del funcionamiento de este algoritmo.

Tabla 1-2 Funcionamiento del algoritmo criptográfico clásico RSA

Parámetros	Datos
Datos Necesarios	p y q, números primos aleatorios de aproximadamente 200 dígitos) n, es la base para la operación módulo

Algoritmo de preparación de Datos	e y d, son números primos las claves pública y privada respectivamente. 1.- Se generan dos números primos grandes aleatorios. 2.- Se calcula el valor de n = p * q. 3.- Se resuelve la expresión phi(n) = (p-1)*(q-1). 4.- e, se obtiene de un proceso aleatorio, dado que: $1 \leq e \leq phi(n)$. 5.-Se obtiene d, dado e * d = 1 mod n
Algoritmo de Cifrado	(dato)^e, se calcula el mod n
Algoritmo de Descifrado	(dato cifrado)^(clave privada), calcula mod n

Fuente: Esquema de algoritmo RSA (Benet, 2015; Saudi, 1998)
Elaborado por: Mantilla Carmen, 2017

2.4.2. Algoritmo Diffie-Hellman

Publicado en 1976, se emplea para realizar un intercambio de claves por un medio no seguro, considerado el primer algoritmo seguro de intercambio de claves anónimas, se usa para el envío de claves cuando pueden ser más de dos destinatarios. Intercambia claves cuando se encripta información considerando que los comunicantes no han establecido contacto previo, comunicándose sin protección. Es una comunicación no confiable, se realiza de manera pública de tal forma que no se puede identificar quien envía el mensaje. Se puede vulnerar mediante el ataque hombre en el medio por lo que autentifica al usuario remitente o receptor, usa el principio del logaritmo discreto (Boneh, 1998). La tabla 2-2, muestra un resumen de su funcionamiento.

Tabla 2-2 Funcionamiento del algoritmo criptográfico clásico Diffie-Hellman

Parámetros	**Datos**
Datos Necesarios	g y p -> son dos números primos grandes (mínimo 300 dígitos, base y modulo respectivamente). a y b, clave secreto de emisor y receptor.
Algoritmo de preparación de Datos	1.- Emisor envía datos g y p. 2.- a y b son números secretos que generan el transmisor y receptor. 3.- El emisor realiza la operación$x = g^a \ mod \ p$ y envía x.

	4.- El receptor realiza la operación $y = g^b \ mod \ p$ y envía el valor de y. 5.- Tanto emisor como receptor intercambian bases Y y X, obtienen la clave genérica para emisor con$C = y^a \ mod \ p$ y para receptor con $C = x^b \ mod \ p$
Algoritmo de Cifrado	C es la llave privada para cifrar información
Algoritmo de Descifrado	Ejecutar las operaciones: $a = \log d_g(x) \ \ y \ \ b = \log d_g(y)$para obtener los números secretos, se considera log d una operación logaritmo discreto.

Fuente: Esquema de algoritmo Diffie-Hellman (Boneh, 1998)
Elaborado por: Mantilla Carmen, 2017

2.4.3. Algoritmo ElGamal

Desarrollado por Taher ElGamal en 1984 es un algoritmo de cifrado asimétrico no posee licencia, se usa en GNU, consta de tres partes el generador de claves y los métodos de cifrado y descifrado. Sirve de algoritmo base para la generación de cifrados como DSS y NIST, la única dificultad radica en que las cadenas de cifrado son muy largas, es menos eficiente y su cómputo es elevado comparado con RSA. Se basa en los principios de Diffie-Hellman y el concepto de los logaritmos discretos, existen dos tipos de algoritmos ElGamal el clásico y el elíptico que usa las curvas elípticas sobre grupos discretos. En la tabla 3-2, se analiza el algoritmo para establecer parámetros de comparación con sus similares (ElGamal, 1985).

Tabla 3-2 Funcionamiento del algoritmo criptográfico clásico ElGamal

Parámetros	**Datos**
Datos Necesarios	Establece un grupo finito sobre p que un número primo grande ->Z_p^*. g es n generador de del cuerpo finito, determinado. x, y, claves aleatorias privadas de los usuario -> 1 <x, y <p. Las claves públicas se generan de las ecuaciones para el algoritmo de obtención de Datos $X = g^x \ mod \ p$y$Y = g^y \ mod \ p$ -> (X, g, p) y (Y, g, p).

Algoritmo de Cifrado	1.- Se divide el mensaje en bloques. 2.- El bloque se representa con un número z, 1 < z < p-1. 3.- el receptor envía su clave pública (Y, g, p). 4.- el emisor genera un número aleatorio k, 1 < k < p-1 enviándolo al receptor. 5.- el emisor envía mensaje codificado: $C = [g^k \ mod \ p, \ M * Y^k \ mod \ p \ ]$
Algoritmo de Descifrado	1.- El receptor recibe el mensaje codificado. 2.- El receptor genera $g^{-ky} \ mod \ p$ con toma el primer elemento $(g^k \ mod \ p)$ 3.- Se descifra aplicando la multiplicación del factor por el segundo elemento del par ordenado

Fuente: Esquema de algoritmo (ElGamal, 1985)
Elaborado por: Mantilla Carmen, 2017

2.4.4. Algoritmo El Rabin

Desarrollado por Michael Rabin en 1979, es considerado el único algoritmo que permitía descifrar un mensaje completo a partir del texto cifrado, se basa en los métodos del teorema chino del resto y la exponenciación modular, se considera más seguro que RSA pero su debilidad está en lo métodos de factorización de las raíces cuadradas que utiliza para generar las claves En la tabla 4-2, se presenta a modo resumen el funcionamiento del algoritmo criptográfico Rabin. (Frances, 2013; Alexi & Chor, 1988).

Tabla 4-2 Funcionamiento del algoritmo criptográfico clásico Rabin

Parámetros	**Datos**
Datos Necesarios	p y q, son las claves privadas. N, es la clave pública.
Algoritmo de preparación de Datos	1.- p y q deben ser primos congruentes en 3 mod 4 y a su vez sus 2 últimos bits deben ser 1 2.- N = p * q.
Algoritmo de Cifrado	1.- C es adquirido 2.-$Z = C^2 \ mod \ n$
Algoritmo de Descifrado	Teorema chino del resto (TCR), p y q son números primos relativos, N tales que mcd(n, m) = 1, dados b_1 y b_2 en Z existe un X tal que: $X \equiv \ b_1 (mod \ n)$

y $X \equiv b_2(mod\ m)$. Pueden existir congruencias un v y w en Z que satisfagan las congruencias: $v \equiv$ w $(mod\ n * m)$.

1.- Utilizando principios del TCR buscamos a y b que satisfagan ap + bp = 1.

2.- Resuelve:

2.1.- $r = c^{(p+1)/4} mod\ p$

2.2.- $s = c^{(q+1)/4} mod\ q$

2.3.- $m_1 = (aps + brq) mod\ n$

2.4.- $m_2 = (aps - brq) mod\ n$

Las raíces son: $m_1, m_2, -m_1\ mod\ n, -m_2\ mod\ n$

Fuente: Esquema de funcionamiento El Rabin (Frances, 2013)
Elaborado por: Mantilla Carmen, 2017

2.5. Criptografía cuántica

La criptografía cuántica es una nueva área dentro de la criptografía, es una combinación de la física cuántica y la técnica de codificación, con el objeto de resolver los problemas que son imposibles o difíciles de resolver con la criptografía clásica. Utiliza las propiedades de la física cuántica como: el teorema de no clonación, el principio de incertidumbre de Heisenberg, y la irreversibilidad de las mediciones cuánticas. Es la primera aplicación comercial de la mecánica cuántica.(García, 2014; Mogos, 2016).

2.5.1. Física cuántica

Conocida como mecánica ondulatoria, estudia el comportamiento de la materia con dimensiones en torno a 1.000 átomos, se complica conocer con exactitud la posición de una partícula, su energía, su posición y velocidad, sin afectar a la propia partícula descrito según el principio de incertidumbre de Heisenberg (Svozil, 2011, Mogos, 2015). Surgió en el siglo XX como respuesta a los problemas que no podían ser resueltos por medio de la física clásica. Son dos los pilares de esta teoría:

- Las partículas intercambian energía en múltiplos enteros de una cantidad mínima posible el quantum de energía.

- La posición de las partículas viene definida por una función que describe la probabilidad de que dicha partícula se halle en tal posición en ese instante (Ciencia, 2006).

Tres tipos son los principales de indeterminismo cuántico que se deben considerar. (Born, 1968, Cochen & Specker, 1969, Calude & Svozil, 2006, Svozil, 2011, Svozil, 2009):

- Indeterminación de los resultados individuales de los eventos individuales propuestos por Born y Dirac.
- Complementariedad cuántica por el uso de variables conjugadas, propuesto por Heidelberg, Pauli y Bohr.
- Valor indefinición debido a Bell, Kochen y Specker y Greenberger, Horne y Zeilinger

2.5.2. Computación cuántica

Es un método en gran parte teórico, que aprovecha las propiedades extrañas de la materia a escalas pequeñísimas para realizar los cálculos más rápidamente que los ordenadores convencionales. El enfoque para la construcción de ordenadores cuánticos es la utilización de fotones que son partículas de luz con propiedades como " superposición " que indica que puede estar en dos estados diferentes al mismo tiempo, en una computadora normal se representa un cero o uno, una partícula cuántica denominado qubit (Mermin, 2002), una cadena de 16 qubits representarían 64.000 números diferentes al mismo tiempo (Ciencia, 2006; Piris, 1999; Born, 1968). Por lo que para cifrar la información se utiliza claves aleatorias generadas con qubits.

2.5.3. Distribución de claves cuánticas

La distribución de clave cuántica, QKD por sus siglas en inglés Quantum key Distribution es una gran aplicación de la mecánica cuántica en las ciencias de la información, garantiza seguridad en el intercambio de la información ya que necesita para la transmisión gran número de bits, para cada qubit recibido correctamente, esto es tolerable para la

distribución de claves, pero no para la comunicación de normal. La QKD depende de las propiedades de los fotones que son vulnerables a la pérdida de señal, inevitable en grandes distancias, pero existen que funcionan a distancias de máximo 100 kilómetros (Pérula, 2011;Chuang, 2000).

2.5.4. Paradoja EPR - Einstein, Podolsky y Rosen

La paradoja EPR es un experimento realizado por Einstein, Podolsky y Rosen que explica la base conceptual del porqué la criptografía cuántica funciona EPR, el principio de localidad establece que los objetos distantes no pueden tener una influencia directa una sobre otra. Esta suposición implica que el resultado de una medición realizada en un objeto no puede influir en las propiedades de otro objeto. El realismo es la idea de que existe una realidad que es independiente del observador, e implica que los objetos tienen propiedades definidas que no son afectados por diferentes tipos de mediciones realizadas en ellos. Estas dos condiciones aparentemente razonables son violadas en el ámbito de la criptografía cuántica (Mogos, 2016).

2.5.5. Teorema de Bell

Prueba la conexión-correlación entre sistemas no relacionados causalmente. El Teorema de Bell afirma "toda teoría de variables ocultas que sea determinista y local tiene necesariamente algunas predicciones incompatibles con la Mecánica Cuántica". Este resultado implica que las teorías deterministas locales de variables ocultas y la Mecánica Cuántica son mutuamente excluyentes (Mogos, 2015). Los protocolos de distribución de claves más recientes se basan en el teorema de Bell. Estos protocolos transmiten las partículas entrelazadas entre un emisor y un receptor, permite comparar sus partículas recibidas y verificar si sus estados cuánticos violan la desigualdad de Bell. Si el grado de violación no es el anticipado, eso significa que el estado cuántico interno es alterado, y la probabilidad de que los espían es muy alta. Esto hace que sea una comunicación segura (Ekert, 1991).

2.5.6. Reconciliación de claves

En sí es un proceso de distribución cuántica de claves donde interviene un emisor, un receptor, un espía y dos canales de comunicación, uno cuántico para enviar fotones y otro clásico para reconciliar y depurar información, determinar si no hay errores en las claves recibidas (Nielsen & Chuang, 2010).

2.6. Algoritmos cuánticos

Dentro de los algoritmos cuánticos se citan los más representativos debido a que presentan diferentes características.

2.6.1. Algoritmo E91

Desarrollado por Artur Ekert en 1991, es un protocolo de distribución de claves basado en el principio de entrelazamiento cuántico (Teorema de Bell), y el uso de pares de fotones EPR. En el experimento utiliza una fuente de fotones EPR, los dos fotones emitidos empiezan siempre en oposición, (Ekert, 1991). Los fotones entrelazados utilizan los estados cuánticos llamados singlet de spin, pueden ser preparados por el transmisor, receptor o algún tercero, y son distribuidos de manera que el transmisor y el receptor tengan un fotón de cada par, como se muestra en el gráfico 1-2.

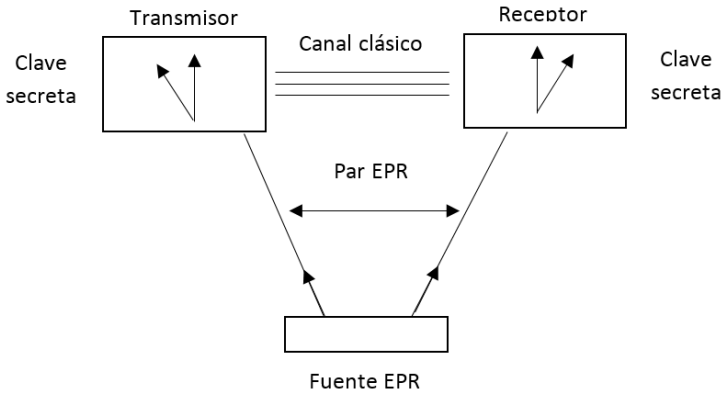

Gráfico 1-2 Protocolo Ekert

Fuente: Ekert, 1991
Elaborado por: Mantilla Carmen, 2017

El entrelazamiento cuántico es la incapacidad para definir el estado cuántico de un objeto sin referenciar al estado cuántico de otro objeto, el cual puede estar o no, alejado espacialmente del primero. Aunque no se pueden establecer conclusiones acerca de los estados individuales de los objetos, el estado cuántico de ambos objetos está bien definido. Las leyes de la mecánica cuántica dan herramientas para el problema de la distribución segura de claves secretas, consiste principalmente en que no se puede extraer información sin revelar su presencia, según las leyes de la mecánica cuántica no es posible copiar estados.

Existen diversos protocolos para la distribución cuántica de claves secretas. En un proceso de distribución cuántica de claves, intervienen un emisor, un receptor y dos canales de comunicación, como se presenta en el gráfico 2-2, uno cuántico para enviar fotones u otras partículas subatómicas y uno clásico que puede se publicó para reconciliar y depurar la información. El transmisor y el receptor usan una parte de su clave para detectar la presencia de intrusos, que puede acceder al canal clásico, como al cuántico y usarlos, pero le restringe la compatibilidad de las leyes de la mecánica cuántica (García, 2014).

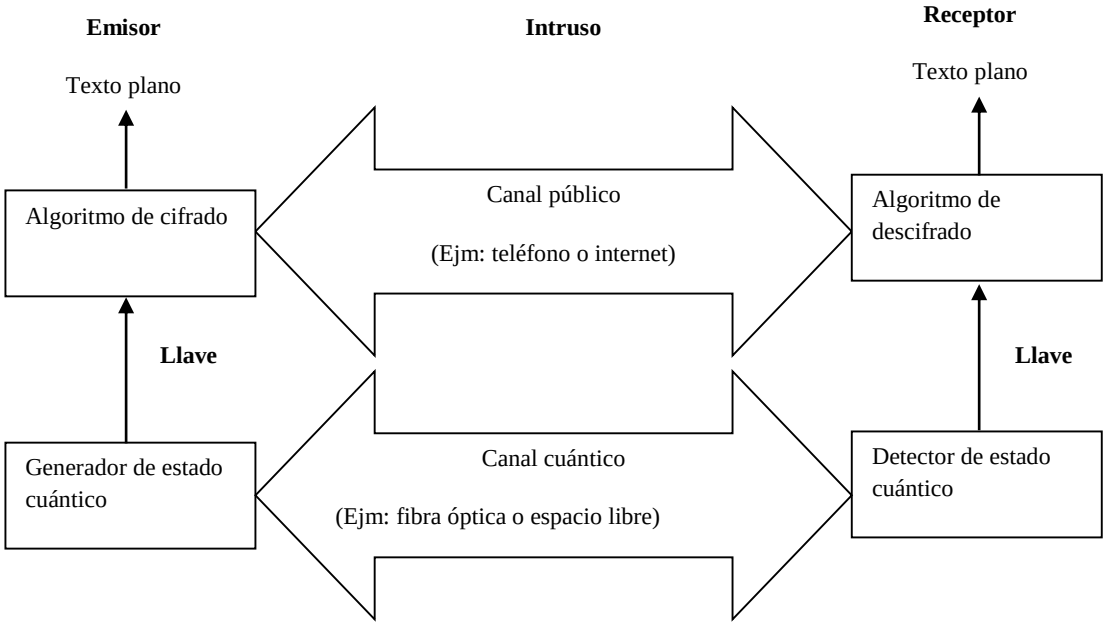

Gráfico 2-2 Modelo de Comunicación Cuántica

Fuente: García, 2014
Elaborado por: Mantilla Carmen, 2017

En la tabla 5-2 se detalla el funcionamiento del protocolo original E91, los datos necesarios para su ejecución en secuencia.

Tabla 5-2 Funcionamiento E91, detalle del proceso de generación e intercambio de claves

Parámetro	Datos
Datos Necesarios	N qubits
Algoritmo de Obtención de Datos	1.- Receptor indica el tamaño de la clave a la fuente.
	2.- La fuente crea los pares entrelazados.
	3.- La fuente envía partículas entrelazadas paralelamente a transmisor y receptor
Algoritmo de Cifrado/Descifrado	1.- El transmisor y el receptor generan una base de forma aleatoria e independiente entre ambos para las partículas recibidas.
	2.- La fuente envía a transmisor y receptor una señal de fin de envío.
	3.- El transmisor y el receptor intercambia sus bases.
	4.- Tanto transmisor como receptor comparan sus bases con la del otro, y se desechan los que no coinciden.
	5.- Se miden las partículas entrelazadas almacenadas en la misma posición que la base tanto en el transmisor como receptor
	6.- Las medidas obtenidas se convierten en clave secreta.

Fuente: Esquema de funcionamiento E91 (Ekert, 1991)
Elaborado por: Mantilla Carmen, 2017

En el gráfico 3-2 y Gráfico 4-2, se muestra el intercambio de bases y de coincidencias para el establecimiento de una QKD entre transmisor y receptor.

Gráfico 3-2 Transmisión de partículas protocolo E91.
Fuente: Ekert, 1991
Elaborado por: Mantilla Carmen, 2017

	Medición 1	Medición 2	Medición 3	Medición 4	Medición 5	Medición 6
Esquema de RX [6]	⊕	⊘	⊖	⊕	⊕	⊘
Particulas de RX	$\|\downarrow\rangle$	$\|\uparrow\rangle$	$\|\downarrow\rangle$	$\|\uparrow\rangle$	$\|\uparrow\rangle$	$\|\downarrow\rangle$
Esquema de TX [6]	⊕	⊘	⊘	⊘	⊕	⊘
Partículas de TX	$\|\uparrow\rangle$	$\|\downarrow\rangle$	$\|\uparrow\rangle$	$\|\downarrow\rangle$	$\|\downarrow\rangle$	$\|\uparrow\rangle$
Coincidencias en las Bases	✓	✗	✗	✗	✓	✓
Clave	0				1	0

Gráfico 4-2 Transmisión de partículas protocolo E91.

Fuente: Ekert, 1991
Elaborado por: Mantilla Carmen, 2017

Para detectar un intruso en la comunicación, el transmisor y receptor comparan las claves rechazadas que no coincidían sus bases. De este modo se comprueba si el intruso ha realizado una medición sobre una de las partículas del par entrelazado, con lo que se rompe las propiedades propias del entrelazamiento (desigualdad de Bell) y se comprueba la presencia de un intruso oportunamente.

2.6.2. Algoritmo BB84

En 1984, Charles Bennett de IBM junto a Gilles Brassard de la Universidad de Montreal, parten del estudio "Codificación Conjugado" de Stephen (Wiesner, 1983), desarrollando el primer codificar cuántico de información clásica, que es un protocolo de distribución de claves, utiliza fotones polarizados, donde el receptor legitimo o ilegitimo, puede recuperar la información con un 100% de confiabilidad, la gráfico 5-2 muestra este protocolo (Bennett, Bessette, Brassard, Salvail & Smolin, 1992).

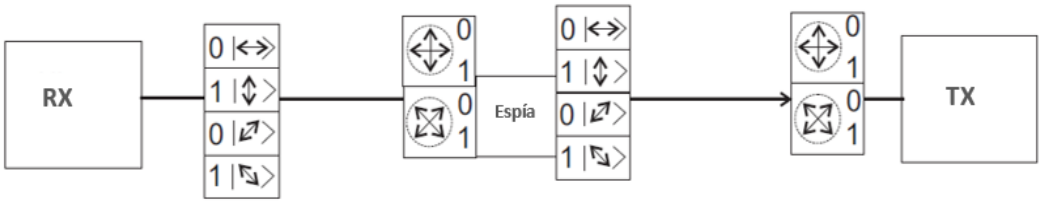

Gráfico 5-2 Protocolo Bennet-Brassard.

Fuente: Bennett, Bessette, Brassard, Salvail & Smolin, 1992
Elaborado por: Mantilla Carmen, 2017

El protocolo de encriptación BB84, está al alcance de la tecnología actual y ofrece la posibilidad de establecer comunicación punto a punto 100% seguras. Para representar los valores de un qubit tenemos de la $|0\rangle$ siguiente forma: $|0\rangle$ y $|1\rangle$, y se pueden expresar mediante las ecuaciones 2.3 y 2.4 respectivamente. Utiliza la base canónica con fotones polarizados verticalmente para representar un $|1\rangle$ y horizontalmente para representar un $|0\rangle$ Pero también utiliza una base transversal, utilizando una polarización de 45° para representar un $|0'\rangle$ y de 135 ° para representar un $|1'\rangle$. Que se puede expresar matemáticamente como se muestra en las ecuaciones 2.5 y 2.6 respectivamente.

$$|0\rangle \stackrel{def}{=} \begin{bmatrix} 1 \\ 0 \end{bmatrix} \tag{2.3}$$

$$|1\rangle \stackrel{def}{=} \begin{bmatrix} 0 \\ 1 \end{bmatrix} \tag{2.4}$$

$$|0'\rangle \stackrel{def}{=} \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \tag{2.5}$$

$$|1'\rangle \stackrel{def}{=} \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \tag{2.6}$$

La tabla 6-2, presenta un resumen de cómo funciona el protocolo BB84, con la secuencia y datos necesarios para que se pueda ejecutar.

Tabla 6-2 Funcionamiento del protocolo BB84

Parámetro	Datos
Datos Necesarios	N qubits
Algoritmo de obtención de datos	1.- El transmisor escoge aleatoriamente la base del qubit a enviar 2.- E l transmisor escoge aleatoriamente el qubit a enviar
Algoritmo de cifrado	1.- El transmisor envía N qubits aleatorios con base aleatoria

Algoritmo de descifrado	1.-El receptor orienta el vidrio polarizado aleatoriamente para leer lo enviado.
	2.- Envían por el canal clásico la polaridad utilizada para leer los qubits ambos conocen que bits fueron compartidos aproximadamente N/2.
	3.- el transmisor selecciona M qubits
	4.- Informa cuales fueron seleccionados por posición no por valor, con lo que construyen una clave K.
	5.- El transmisor envía m, m[i] $\oplus$ K[i]
	6.- Receptor extrae m con la llave K

Fuente: Esquema de funcionnameinto de BB84, Bennett, Bessette, Brassard, Salvail &Smolin, 1992
Elaborado por: Mantilla Carmen, 2017

El transmisor y el receptor necesitan un protocolo que garantice que con 3/4 partes de la llave no sea posible reconstruir el mensaje, de esta forma si el transmisor recibe basura se concluirá que hay un intruso escuchando el canal. Si un grupo de intrusos escuchan el canal las veinte y cuatro horas del día no se podría transmitir, pero sabemos que están ahí, lo que se puede resolver usando un canal secundario para el intercambio de clave, pero no es posible que se acceda sin darnos cuenta.

2.6.3. Algoritmo E92

Ivanovic demostró en 1987, que dos estados cuánticos no ortogonales pueden ser distinguidos sin ambigüedad, pero se añaden pérdidas al sistema. B92 es un protocolo para la generación e intercambio cuántico de claves basado en BB84, que representa los bits 0 y 1, como se muestra en la gráfico 6-2, (Bennett, 1992). Se diferencia de BB84 porque utiliza solo un estado no ortogonal en cada base complementaria en lugar de dos, con lo que en total resultan dos polarizaciones en lugar de cuatro y no se necesita la reconciliación de las bases, porque el receptor distingue sin ambigüedad cuando eligió la base correcta.

BIT	ESTADO
0	$\|\rightarrow\rangle \equiv \|0\rangle$
1	$\|\nearrow\rangle \equiv \|1'\rangle$

Gráfico 6-2 Notación B92.

Fuente: Bennett, 1992
Elaborado por: Mantilla Carmen, 2017

Para entender este protocolo es conveniente estudiar la implementación de la detección de estados de polarización en el transmisor, que se presenta en el Gráfico 7-2. Al igual que en BB84, el transmisor codifica los bits de la clave en estados de polarización lineales y forma un ángulo relativo de 45˚ entre sí. En el transmisor se elige aleatoriamente la base para medición. El divisor de haz al 50 % modela la elección aleatoria, un fotón único irá por el camino de transmisión o el de reflexión con una probabilidad del 50 % por vez, sin tener en cuenta la polarización incidente. Se dispone polarizadores lineales antes de los detectores con una diferencia de orientación de 45˚ entre ambos y a 90˚ de los estados transmitidos. Con esto se asegura que el estado recibido es el polarizado a 45˚ de la orientación del analizador previo a ese detector, ya que el polarizador a 90˚ de dicho analizador es bloqueado (Herreros, 2004; Bautista, 2015; García, 2014).

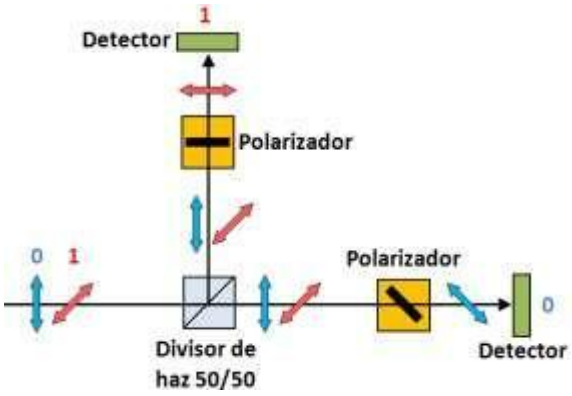

Gráfico 7-2 Detección de fotones en B92.

Fuente: Bennett, 1992

Con lo que cada vez que se recibe un fotón utilizando B92, se puede asegurar que se realizó una medida en la base correcta; por eso en B92 no existe reconciliación de bases y la clave intercambiada será directamente la clave depurada. Por el canal público se

intercambia una fracción de la clave verificando para cada instante que el bit codificado es idéntico y admitiendo también un cierto valor límite para el QBER para detectar la presencia de un espía. La fracción de bits que se pueden distinguir sin ambigüedad en transmisor es $1 - \cos(\alpha)$, donde α es el ángulo entre ambos estados, que para el caso de 45˚ es del 29 %. A B92 se puede aplicar un ataque a la seguridad llamado "ambiguous state discrimination", donde si las pérdidas del canal superan el 71 %, un intruso puede pasar desapercibido si compensara las pérdidas que introduce estableciendo un canal sin ruido entre el intruso y el receptor. Por lo que este protocolo exige un análisis correcto de pérdidas para eliminar la clave la información extraída por el atacante. La tabla 7-2, presenta un resumen del funcionamiento del protocolo B92.

Tabla 7-2 Funcionamiento del protocolo B92

Parámetro	Datos
Datos Necesarios	N qubits
Algoritmo de Obtención de Datos	1.- El transmisor codifica los bits de la clave con estados de polarización lineales y formando un ángulo relativo de 45˚ entre sí.
Algoritmo de Cifrado	Envía N qubits aleatorios
Algoritmo de Descifrado	1.- Antes de los detectores se disponen polarizadores lineales con una diferencia de orientación de 45˚ entre ambos y a 90˚ de los estados transmitidos 2.- El receptor elige aleatoriamente la base de medición. 3.- Se recibe la clave depurada

Fuente: Esquema de funcionamiento E92, (Bennett, 1992)
Elaborado por: Mantilla Carmen, 2017

2.7. Complejidad computacional

La teoría de la complejidad de los algoritmos permitirá, conocer la fortaleza de un algoritmo para saber su vulnerabilidad computacional (COOK, 1983; Fortnow & Homer, 2002).

Un modelo de computación se basa en, definir sintácticamente los procedimientos que se consideraran como mecánicos en el algoritmo o modelo; definir semánticamente como se van a ejecutar los procedimientos y establecer qué se entiende por resolver un problema en el modelo, cual es el modo de computación para aceptar un dato de entrada. Es modelo es posible diseñar dispositivos que permitan simular la ejecución de los procedimientos del modelo estas pueden ser dispositivos reales, teóricos o abstractos.

2.8. Algoritmos óptimos

Para resolver un problema se ejecuta un algoritmo computacional se consumen recursos del computador es importante estimar estos los recursos como son memoria, espacio, tiempo, etc., con el fin de que el computador no se cuelgue por el uso de sus recursos, el concepto de mejor solución estar referido a una cierta medida de complejidad que cuantifique los recursos. Para determinar un algoritmo óptimo que resuelve un determinado problema debemos considerar: determinar una cota inferior asintótica de la cantidad de recursos que necesita para su ejecución cualquier algoritmo que resuelva dicho problema y hallar un algoritmo que resuelva el problema con la cantidad de recursos que utiliza es del orden exacto de la cota inferior, un algoritmo óptimo que resuelve un problema, tiene relación con la obtención de problemas irresolubles algorítmicamente: se debe hallar un algoritmo que satisfaga una propiedad que implica a todos los algoritmos que resuelven dicho problema.

CAPÍTULO III

3. DISEÑO DE INVESTIGACIÓN

En este capítulo se determinó el diseño de la investigación en donde se estableció un análisis comparativo de los algoritmos criptográfico clásicos y los algoritmos cuánticos en la seguridad de la obtención de la clave criptográfica, se tomó como punto de inicio el análisis del estudio del arte sobre algoritmos criptográficos clásicos y cuánticos, la operacionalización de las variables así como las técnicas e instrumentos que permitieron determinar los parámetros de comparación para obtener resultados generales de la investigación.

Para la investigación se determinó un diseño no experimental transversal descriptivo, ya que se buscó indagar la incidencia de los valores que se manifiestan en las variables, luego se estableció una sustentada comparación entre algoritmos clásicos vs cuánticos. Los últimos son los más adecuados para la seguridad en la obtención de claves.

3.1. Tipo de investigación

La investigación fue mixta, ya que utilizó datos cualitativos y cuantitativos; descriptiva debido a que se estudió cada uno de los algoritmos de criptografía clásica y cuántica con la finalidad de determinar comparaciones respecto a su seguridad en la obtención de claves. De tipo documental ya que realizó un estudio del arte y básica ya busca acrecentar conocimientos teóricos más que prácticos.

3.2. Métodos de investigación

Para el desarrollo de este proyecto se trabajó con una triangulación de métodos, el primero de ellos él es analítico, en el que se separó varios aspectos de los algoritmos criptográficos tanto clásicos como cuánticos para determinar su eficiencia con relación a la seguridad

en la obtención de claves. En segunda instancia se utilizó el método inductivo, que bajo criterios teóricos demostró que los algoritmos BB84, B92 y E91 son más eficientes al momento de impedir la obtención de claves, esto llevó a inducir que los algoritmos criptográficos cuánticos pueden ser más eficientes para la seguridad en la obtención de clave. Y se aplicó estadística no paramétrica para demostración de hipótesis generada.

3.3. Técnicas de recopilación de la información.

Se empleó como técnica principal la revisión de bibliográfica, análisis de contenidos y que permitió obtener la información necesaria acerca de los algoritmos clásico y cuánticos y mediante un análisis determinar los resultados de la investigación que fue la comparación en la seguridad en la obtención de claves criptográficas.

3.4. Hipótesis de la Investigación

En la investigación se definió en el primer capítulo la hipótesis de esta investigación y se genera su hipótesis nula:

H_1: "Los algoritmos criptográficos cuánticos son más adecuados para la seguridad en la obtención de clave que los algoritmos clásicos".

H_0: "Los algoritmos cuánticos **NO** son los más adecuados para la seguridad en la obtención de clave que los algoritmos clásicos".

3.5. Tipo de variables

Para definir los resultados de la comparación entre algoritmos criptográficos vs cuánticos se definieron los tipos de variables, además se realizará la operacionalización conceptual y metodológica de las variables con la finalidad de estandarizar el estudio investigativo.

Analizando la hipótesis se determinó las siguientes variables para el estudio:

Variable Independiente: Algoritmos de criptográfico.

Variable Dependiente: Seguridad en la obtención de claves.

Entonces se dice que la seguridad en la obtención de claves depende únicamente de los algoritmos criptográficos utilizados en la transmisión con lo cual se da cumplimiento al modelo de diseño no experimental transversal.

3.6. Operacionalización de las variables

Al realizar la operación conceptual de las variables de la hipótesis se define el criterio con el cual el investigador realiza su análisis, la operacionalización conceptual define que se entiende por el tipo de variable para que no existan confusiones en su papel en la hipótesis y la operacionalización metodológica determina la forma en las que estas serán medidas sus indicadores e índices, los indicadores son cifras que son obtenidas al haber realizado una medición y permiten mantener un ámbito de control.

3.7. Operacionalización Conceptual

Al cumplir con los criterios de la operacionalización de variables y teniendo las variables dependientes e independientes se realizará la siguiente generalización de conceptos para definir obtener una comparación de algoritmos criptográficos clásicos vs cuánticos en la seguridad de obtención de clave y la operacionalización se presenta en la tabla 8-3.

Tabla 8-3 Operacionalización Conceptual de las Variables

VARIABLE	TIPO	CONCEPTO
Algoritmo criptográfico	Independiente	Algoritmo para modificar los datos de un documento para asegurar lo transmitido.
Seguridad en la obtención de clave	Dependiente	Dificultad de interceptar la información en un ataque.

Fuente: Revisión bibliográfica
Elaborado por: Mantilla Carmen, 2017

Con esta operacionalización se define un algoritmo criptográfico como un "algoritmo para modificar los datos de un documento para asegurar lo transmitido" y conceptualización matemática con lo que se pudo definir la operacionalización metodológica.

3.8. Operacionalización Metodológica Variable Independiente

Al realizar la operación metodológica de las variables se estable los indicadores e índices que nos permitirán evaluar la variable y obtener resultados a partir de las mediciones, este proceso se realizó mediante descripciones de tablas en donde se ingresan la hipótesis, la variable y su tipo, los indicadores, índices, técnicas e instrumentos de medición de la siguiente manera como se muestra en la tabla 1-3:

Tabla 1-3 Operacionalización metodológica variable independiente

Variable independiente	Dimensión	Indicador	Técnicas	Instrumento
Algoritmo criptográfico	Datos de Entrada	Número de datos de entrada. Dificultad para la preparación de datos.	Revisión bibliográfica	Fichas bibliográficas Ficha de análisis de contenido

	Algoritmo de Cifrado/ Descifrado.	Número de pasos. Número de definiciones matemáticas.	Análisis de contenidos
	Complejidad	Número de estructuras	

Fuente: Revisión bibliográfica
Elaborado por: Mantilla Carmen, 2017

La variable se dividió en los:

Datos de Entrada.- Son los parámetros definidos en el capítulo 2 de los algoritmo criptográfico que permiten que se realicen los algoritmos de cifrado y descifrado como la clave de usuario y mensaje cifrado transmitido.

Número de Datos de Entrada.- Este índice hace referencia al número de datos completo que requiere el algoritmo para su funcionamiento, el total de número de claves más el mensaje cifrado.

Dificultad para la preparación de los datos.- El índice controla la cantidad de procesos matemáticos (cálculos y conceptos matemáticos que los generan) que se deben aplicar a un dato de entrada para que éste sea considerado como útil para el algoritmo de cifrado o des cifrado.

Algoritmo de Cifrado/Descifrado.- Es el método por el cual el algoritmo criptográfico cifra/descifra la información antes de ser transmitida, el algoritmo usa datos de entrada su totalidad o parcialmente, el algoritmo de cifrado no necesita la clave privada del receptor en criptosistemas de clave pública, analógicamente el mismo procedimiento se produce en el algoritmo de des cifrado.

Número de pasos.- El índice determina la cantidad de procedimientos que debe realizar el algoritmo para cifrar la información en claro desde el ingreso de la información hasta la salida del texto cifrado.

Dificultad de los pasos.- El índice determinar la dificultad de un paso de ejecución del algoritmo de cifrado en contraste a los conceptos matemáticos que se emplean para dicho procedimiento.

Complejidad.- La complejidad del algoritmo relaciona la cantidad de estructuras del algoritmo, por lo tanto, es un valor que recibe el algoritmo con respecto al tiempo de encriptación.

Número de estructuras.- se refiere a la estructuras de decisión, bucles de repetición y condicionales que se utilizan en el algoritmo.

3.9. Operacionalización Metodológica Variable Dependiente

Esta operacionalización se pretende definir las preguntas que se busca para determinar el mejor algoritmo criptográfico para brindar seguridad, lo que se presenta en la tabla 2-3.

Tabla 2-3 Operacionalización metodológica de la variable dependiente

Variable dependiente	Dimensión	Índices	Técnica	Instrumento
Seguridad en la obtención de clave	Aplicabilidad	Tecnología aplicada en el mercado	Revisión bibliográfica Análisis de contenidos	Fichas bibliográficas Ficha de análisis de contenido
	Fortaleza del algoritmo	Origen de a clave Base de la seguridad Unidad de estructura de la información Detección de intrusos El atacante copia la información		

Fuente: Revisión bibliográfica
Elaborado por: Mantilla Carmen, 2017

Aplicabilidad.-es de importancia considerar esta categoría ya que no tendría importancia el estudio si no hay la factibilidad de que se implemente en un medio real.

Tecnología aplicada en el mercado.- Este índice indicará cualitativamente la utilización en el medio de los algoritmos criptográficos.

Fortaleza del algoritmo.- Existen parámetros que identifican la fortaleza en la seguridad de la obtención de la clave, este conjunto de características determinan cuan inviolable es su seguridad.

Origen de la clave.- la clave es código secreto de cierta longitud que se utiliza para cifrar o descifrar la información que será transmitida. El origen se determina con el método con la que fue creada la clave.

Base de la seguridad.- en que se apoya para brindar la seguridad en la obtención de la clave.

Unidad de estructura de la información.- las bondades que ofrece su unidad estructural para la seguridad en la obtención de clave.

Detección de intrusos.- la capacidad de detectar si un intruso se encuentra escuchando el canal de transmisión y poder tomar medidas al respecto.

El atacante copia la información.- Si al realizarse una intercepción, al ser violada la seguridad del canal el atacante puede copiar la información y utilizarla posteriormente para malos fines.

3.10. Comparación de los algoritmos

Para realizar la comparación de los algoritmos se estableció tres fases importantes para el desarrollo de la investigación.

En la primera fase determinamos concretamente los parámetros bajos los que van a ser comparados los algoritmos del mismo grupo tanto clásico como cuántico, en base a una revisión bibliográfica sistemática de los algoritmos criptográficos clásicos para distribución de clave, se seleccionó cuatro algoritmos para el grupo y se realizó una síntesis de las características más relevantes como: número de datos de entrada, número de pasos algoritmo cifrado/descifrado, número de operaciones matemáticas de los cuales para ponderar porcentualmente se estima sobre el total del valor de la variable y los índices dificultad en las operaciones para preparación de datos de entrada, orden de complejidad son de variables cualitativas respecto a lo indicado en la teoría, y la tienen valoraciones de bajo, medio bajo, medio, medio alto y alto. De manera similar se

seleccionó tres algoritmos cuánticos con los índices: número de pasos algoritmo cifrado/descifrado el cual es cualitativo y tiene trato similar al de los clásicos y los índices número de datos de entrada, dificultad en las operaciones para preparación de datos de entrada, orden de complejidad son variables cualitativas. Al analizar los resultados de las variables se pudo tomar la decisión sobre el más adecuado de cada grupo.

En una segunda del desarrollo de esta investigación se obtuvo los índices para comparar los algoritmos cuánticos con los clásicos con respecto a la seguridad en la obtención de clave, los cuales fueron: unidad estructural de información, base de la seguridad, origen y tamaño de la clave, el atacante copia la información, detección de intrusos y tecnología aplicada que en el estudio los define de naturaleza cualitativa, con las valoraciones antes indicadas.

En una tercera fase se realiza la evaluación de los resultados obtenidos para la comprobación de la hipótesis de la investigación aplicando el estadístico CHI Cuadrado.

3.11. Alcance de la investigación

El presente trabajo de investigación da a conocer las ventajas de los algoritmos criptográficos cuánticos sobre los clásicos en la seguridad en la obtención de clave criptográfica sustentando teóricamente mediante una revisión sistemática, donde determina índices para compararlos, establece cuales son los más apropiados para este propósito y propone un estudio requerimientos técnicos y económicos para una propuesta de implementación de criptografía cuántica en Ecuador, el estudio es teórico por que no se incluirán pruebas.

Para el estudio del arte se está aplicando revisión sistemática, metodología hoy en día implementada para la realización de estudios de revisión bibliográfica, se considera relevante su implementación, esta revisiones tienen como objetivo presentar una evaluación justa de un tema de investigación utilizando una metodología confiable, rigurosa y auditable (Kitchenham & Charters, 2007).

CAPÍTULO IV

4. RESULTADOS Y DISCUSIÓN

En esta sección se presenta los resultados obtenidos de los procesos realizados para obtener determinar el algoritmo criptográfico más adecuado para la seguridad en la obtención de clave, según la metodología aplicada descrita en el capítulo anterior.

4.1 Ventajas y desventajas de los algoritmos criptográficos cuánticos vs clásicos

Del análisis en el estudio realizado se presentan las ventajas y desventajas más relevantes de los algoritmos criptográficos cuánticos frente a los clásicos en la seguridad de la obtención de claves.

Ventajas

- Cada día la tecnología avanza y con el tiempo permitirá utilizar dispositivos cuánticos que brinde seguridad teóricamente 100%.
- Posee varios métodos efectivos para detección de los posibles ataques lo que garantiza la seguridad de la distribución de claves cuánticas.
- Utiliza claves totalmente aleatorias (QKD) a nivel de hardware basadas en la mecánica cuántica por lo que no son predecibles como en la criptográfica clásica que utiliza claves pseudo aleatorias generadas por un simple algoritmo numérico.
- Utiliza partículas de luz, una partícula cuántica denominado qubit que tiene la propiedad de estar en dos estados diferentes al mismo tiempo, mientras que en la clásica pueden representar un cero o uno, lo que con una misma cadena de qubits podría representar números diferentes al mismo tiempo.
- La clave no se puede copiar ya que cumple el principio de incertidumbre de Heisenberg que dice que al hecho de medir un sistema cuántico perturba el sistema descartando la

posibilidad de interceptación, mientras que en los clásicos se pueden copiar y aunque todavía no haya computadores con capacidades de descifrar algunos códigos la computación cuántica es una amenaza para la criptografía clásica ya que son capaces de resolver problemas de factorización, problemas de logaritmo discreto que son las bases matemáticas de los algoritmos clásicos provocando crisis social y económica.

- Las claves pueden ser transmitidas también en un canal normal.

Desventajas

- Al momento debido a que la tecnología para los dispositivos cuánticos transmisores y receptores tiene imperfecciones y son experimentales no ofrecen seguridad al 100% permitiendo algunos ataques a la distribución de claves cuánticas.
- No se comercializan ampliamente y algunos son experimentales, en los clásicos existe tecnología hardware y software desarrollados en producción y aplicados masivamente.
- Las aplicaciones comerciales no experimentales trabajan máximo para una distancia de 100 Km.

4.2. Selección del algoritmo criptográfico clásico

A continuación se presentan los resultados de los índices estudiados para seleccionar el algoritmo más representativo del grupo de los algoritmos criptográficos clásicos para la seguridad en la obtención de clave.

4.2.1. Índice número de datos de entrada

En la tabla 1-4, se presenta los resultados del índice número de datos, donde se debe considerar que a mayor número de datos el algoritmo es más fuerte.

Tabla 1-4 Índice número de datos de entrada

Algoritmo	Número de Datos de Entrada	Ponderación
RSA	5	0.313
Diffie-Hellman	4	0.250
El Rabin	4	0.250
ElGamal	3	0.188
Total	**16**	**1.000**

Fuente: Revisión bibliográfica
Elaborado por: Mantilla Carmen, 2017

4.2.2. Índice número de pasos algoritmo cifrado/descifrado

Para encriptar y desencriptar el texto en claro se deben seguir los pasos propios del algoritmo criptográfico debido que si no se aplican de la forma estipulada no se obtiene el resultado esperado, para la comparación se determinó los siguientes pasos en los algoritmos de cifrado/des cifrado. El resultado del análisis de este índice se presenta en la Tabla 2-4.

Tabla 2-4 Índice número de pasos algoritmo cifrado/descifrado

Algoritmo	Número de Pasos algoritmo cifrado/descifrado	Ponderación
RSA	2	0.125
Diffie-Hellman	2	0.125
El Rabin	4	0.250
ElGamal	8	0.500
Total	**16**	**1.000**

Fuente: Revisión bibliográfica
Elaborado por: Mantilla Carmen, 2017

4.2.3. Índice Operaciones Matemáticas

En los algoritmos criptográficos es de importancia conocer de donde provienen sus componentes, como funcionan, sus fortalezas y debilidades con la finalidad de usarlos correctamente o fortificarlos por lo que sé cuantificó la cantidad de conceptos matemáticos que necesita cada algoritmo. Los resultados se presentan en la Tabla 3-4.

Tabla 3-4 Índice operaciones matemáticas usadas

Algoritmo	Operaciones matemáticas	Número de operaciones matemáticas	Ponderación
RSA	Números Primos Algoritmo de Euclides Aritmética Modular	3	0.1875
Diffie-Hellman	Números Primos Aritmética Modular Logaritmos	3	0.1875
El Rabin	Número Compuesto Número Primos Congruentes Teoría de Números Teorema Chino del Resto Algoritmo Extendido de Euclides	5	0.3125
ElGamal	Número Primos Primos Fuertes Grupos Finitos Aritmética Modular Algoritmo Extendido de Euclides	5	0.3125
	Total	**16**	**1.0000**

Fuente: Revisión bibliográfica
Elaborado por: Mantilla Carmen, 2017

4.2.4. Índice dificultad en las operaciones para preparación de datos de entrada

El indicador se analizó ya que los datos de entradas serán preparados aplicando operaciones matemáticas para aplicar el algoritmo de encriptación, agregando dificultada para la obtención de la claves con un valor cualitativo como se muestra en la Tabla 4-4.

Tabla 4-4 Índice dificultad en las operaciones para preparación de datos de entrada

Algoritmo	Dificultad en las operaciones para preparación de Datos de Entrada	Valoración
RSA	Multiplicación y Módulo	Alta
Diffie-Hellman	Potencia y Módulo	Alta
El Rabin	Congruencia de números primos	Media
ElGamal	Grupos finitos	Baja

Fuente: Revisión bibliográfica
Elaborado por: Mantilla Carmen, 2017

4.2.5. Índice Orden de Complejidad

El orden de complejidad del algoritmo se define por la cantidad de estructuras de decisión como los if, estructuras anidadas, multi condicional, switch y bucles de repetición como while, do while, for, lo que se obtuvo se presenta en la tabla 5-4.

Tabla 5-4 Índice orden de complejidad

Algoritmo	Valoración cualitativa orden de Complejidad
RSA	Alta
Diffie-Hellman	Alta
El Rabin	Medio
ElGamal	Alta

Fuente: Revisión bibliográfica
Elaborado por: Mantilla Carmen, 2017

4.2.6. Resumen comparativo de índices para algoritmos criptográficos clásicos

El resumen de los índices estudiados para la seguridad en la obtención de clave de los algoritmos criptográficos clásicos se presentan en las tablas 6-4 y Tabla 7-4 debido a que son de diferente naturaleza los índices analizados.

Tabla 6-4 Resumen de análisis de índices cuantitativos de los algoritmos criptográficos clásicos

Algoritmo	Número de Datos de Entrada	Número de Pasos algoritmo cifrado/descifrado	Número de Operaciones Matemáticas	Total
RSA	0.313	0.125	0.1875	0.208
Diffie-Hellman	0.250	0.125	0.1875	0.188
El Rabin	0.250	0.250	0.3125	0.271
ElGamal	0.188	0.500	0.3125	0.333

Fuente: Revisión bibliográfica
Elaborado por: Mantilla Carmen, 2017

Tabla 7-4 Resumen de análisis de índices cualitativos de los algoritmos criptográficos clásicos

Algoritmo	Dificultad en las operaciones para preparación de datos de entrada	Orden de Complejidad
RSA	Alta	Alta
Diffie-Hellman	Alta	Alta
El Rabin	Media	Media
ElGamal	Baja	Alta

Fuente: Revisión bibliográfica
Elaborado por: Mantilla Carmen, 2017

El resumen de los índices cuantitativos estudiados para la seguridad en la obtención de clave de los algoritmos criptográficos clásicos se presentan en la Gráfico 1-4, como se puede observar el de más peso es ElGamal.

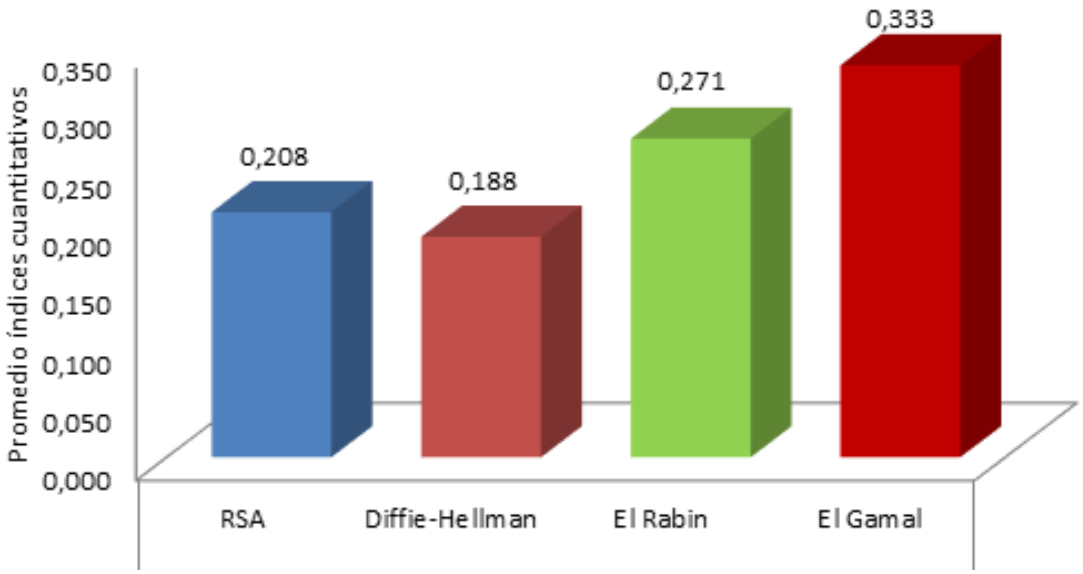

Gráfico 1-4 Valoración de índices cuantitativos algoritmos criptográficos clásicos

Fuente: Análisis de índices
Elaborado por: Mantilla Carmen, 2017

En el Gráfico 2-4., se muestra el resumen comparativo de los índices cualitativos que se consideraron para la selección del algoritmo más óptimo del grupo de los algoritmos clásicos para la seguridad de obtención de clave, como se puede observar los de más peso son RSA y Diffie-Hellman.

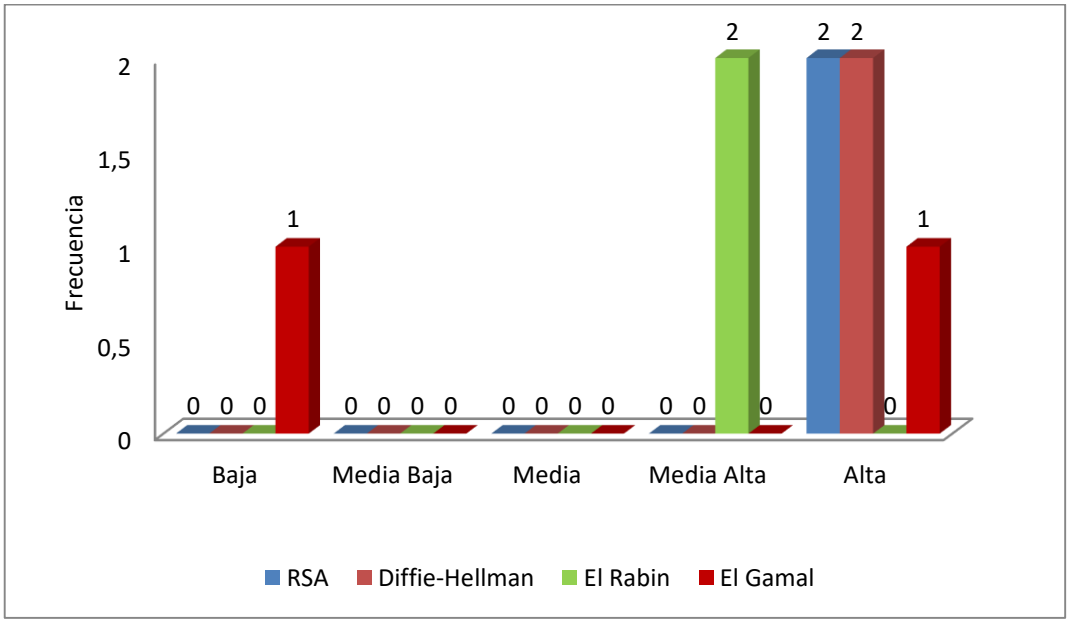

Gráfico 2-4 Valoración de índices cualitativos algoritmos criptográficos clásicos

Fuente: Análisis de índices
Elaborado por: Mantilla Carmen, 2017

Aunque ElGamal sea el más alto en los índices cuantitativos se descarta como el más representativo del grupo de los algoritmos criptográficos clásicos debido a que en los índices cualitativos es el más bajo, posterior a este se analizó el algoritmo RSA que es el segundo en cuanto al valor de los índices cuantitativos y en los cualitativos es uno de los más altos por lo que se consideró como el más representativo de este grupo.

4.3 Selección del algoritmo cuántico de distribución de clave para la comparación

En la esta sección se muestra los resultados de los índices estudiados para seleccionar del representante del grupo de los algoritmos criptográficos cuánticos como el más fuerte para la seguridad en la obtención de la clave.

4.3.1 Índice número de datos de entradas

La tabla 8-4 muestra los resultados con respecto al índice número de entrada de datos para los algoritmos criptográficos cuánticos, como se puede observar el valor de la entrada de datos es un valor aleatorio N con lo al querer adquirir un atacante la clave, este no sabría si la obtuvo en su totalidad, por lo que se califica cualitativamente con alto con respecto a la seguridad en la obtención de clave.

Tabla 8-4 Índice número de datos de entrada

Algoritmo	Número de Datos de Entrada	Valoración cualitativa
BB84	N	Alta
B92	N	Alta
E91	N	Alta

Fuente: Revisión bibliográfica
Elaborado por: Mantilla Carmen, 2017

4.3.2 Dificultad en preparación de datos entrada

La Tabla 9-4, se presentan los resultados obtenidos con respecto al índice dificultad en las operaciones para preparación de datos de entrada, medido para los algoritmos criptográficos cuánticos.

Tabla 9-4 Índice dificultad en las operaciones para preparación de datos de entrada

Algoritmo	Dificultad en las operaciones para preparación de Datos de Entrada	Valoración cualitativa
BB84	Selección aleatoria de polarización, qubit y tamaño.	Alta
B92	Selección aleatoria de polarización, qubit y tamaño	Alta
E91	Creación de N pares entrelazados indicado por el transmisor y paralelo de partículas entrelazadas a transmisor y receptor.	Alta

Fuente: Revisión bibliográfica
Elaborado por: Mantilla Carmen, 2017

4.3.3 Orden de complejidad

Uno de los parámetros importantes para evaluar uno de los algoritmos criptográficos cuánticos es el orden de complejidad, los resultados de este análisis se presentan en la tabla 10-4, como se puede observar la complejidad en los algoritmos criptográficos cuánticos son similares.

Tabla 10-4 Índice orden de complejidad

Algoritmo	Orden de Complejidad	Valoración cualitativa
BB84	Fotones polarizados ortogonales	Alta
B92	Fotones polarizados no ortogonales	Alta
E91	Fotones entrelazados	Alta

Fuente: Revisión bibliográfica
Elaborado por: Mantilla Carmen, 2017

4.3.4 Pasos algoritmo de cifrado

La tabla 11-4, presenta los resultados del índice número de pasos algoritmo cifrado/descifrado que se utilizó como parte de los parámetros de selecciona para el representante de este grupo.

Tabla 11-4 Índice número de pasos algoritmo cifrado/descifrado

Algoritmo	Número de Pasos	Ponderación
BB84	7	0.412
B92	4	0.235
E91	6	0.353
Total	**17**	**1.000**

Fuente: Revisión bibliográfica
Elaborado por: Mantilla Carmen, 2017

4.3.5 Resumen análisis índices de algoritmos criptográficos cuánticos

En las tablas 12-4, se muestra un resumen de los resultados del análisis de los índices cuantitativos para la selección del algoritmo más representativo para el grupo de los algoritmos criptográficos cuánticos.

Tabla 12-4 Resumen de análisis de índices cualitativos de los algoritmos criptográficos cuánticos

Algoritmo	Promedio cuantitativo
BB84	0.412
B92	0.235
E91	0.353

Fuente: Revisión bibliográfica
Elaborado por: Mantilla Carmen, 2017

Del estudio realizado se presentan los resultados de los índices cuantitativos en el gráfico 3-4., para tomar una decisión según un análisis el representante de este grupo de acuerdo

al conjunto de mejores características presentadas, como se puede observar el de mayor peso es BB84.

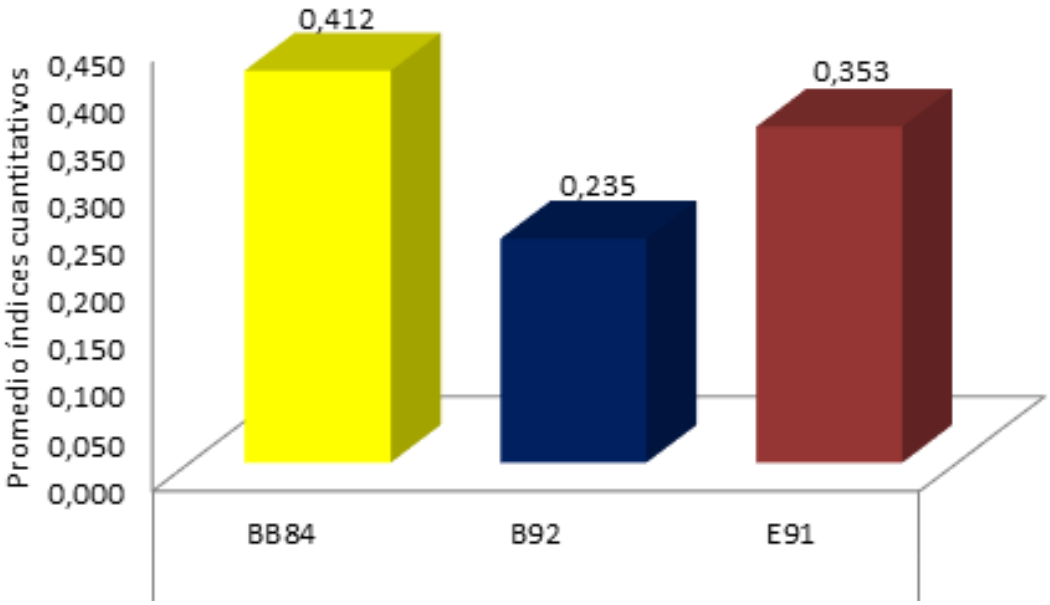

Gráfico 3-4 Valoración índices cuantitativos algoritmos criptográficos cuánticos

Fuente: Análisis de índices
Elaborado por: Mantilla Carmen, 2017

En el gráfico 4-4., se presenta un resumen comparativo del conjunto de parámetros cualitativos que se han medido para seleccionar el mejor algoritmo criptográfico cuántico para la seguridad en la obtención de clave, como se puede observar tienen similares pesos.

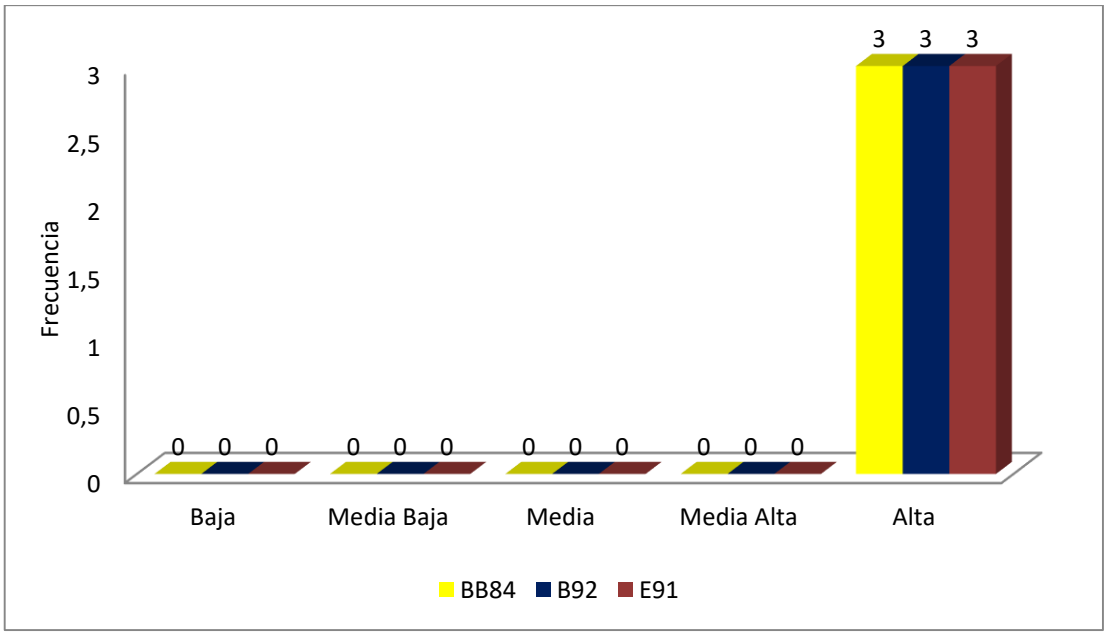

Gráfico 4-4 Valoración índices de algoritmos criptográficos cuánticos

Fuente: Análisis de índices
Elaborado por: Mantilla Carmen, 2017

Debido a que en los indicies cualitativos son similares, el mayor peso en los índices cualitativos es el que determina que BB84 es el algoritmo criptográfico cuántico más representativo de este grupo.

4.4 Comparación del algoritmo criptográfico clásico RSA y el algoritmo criptográfico BB84 en seguridad de obtención de clave

Se analiza las características más relevantes del algoritmo tanto clásico como cuántico para determinar los parámetros bajo los que pueden ser comparados y a cada indicador se le da una valoración ya sea cualitativa o cuantitativa.

4.4.1 Índice unidad estructural de información

Una de las características que determina la fortaleza del algoritmo clásicos vs los cuánticos es que en los cuánticos el qubit tiene la propiedad de estar en dos estados diferentes al mismo tiempo y en la clásica el bit puede representar un cero o uno. Por lo

que se determina una valoración alta al uso de qubit y media a los bits. Los resultados con respecto a este índice se presentan en la tabla 13-4.

Tabla 13-4 Índice análisis comparativo unidad estructural de información

Nombre del algoritmo	Unidad estructural de información	Valoración cualitativa
Algoritmo criptográfico clásico RSA	Bit	Media
Algoritmo criptográfico Cuántico BB84	Qubit	Alta

Fuente: Revisión bibliográfica
Elaborado por: Mantilla Carmen, 2017

4.4.2 Índice base de la seguridad

Las características que determina la seguridad de obtención de la clave es en sí en que se basa la seguridad de algoritmo, mientras que en los clásicos depende del tamaño, de que la clave sea secreta y de la fortaleza del algoritmo para que aunque sea copiado la clave no se pueda descifrar en un largo periodo de tiempo; por lo que se considera la seguridad en la que se basa los algoritmos de criptografía clásica media alta y los cuánticos alto ya que no se puede descifrar. La tabla 14-4, presenta los resultados obtenidos de este índice.

Tabla 14-4 Índice base de la seguridad

Nombre del algoritmo	Base de la seguridad	Valoración cualitativa
Algoritmo criptográfico clásico RSA	En la complejidad del algoritmo matemático, la clave de cifrado y el supuesto de que el presunto espía no puede resolver un problema computacional difícil.	Media Alta
Algoritmo criptográfico Cuántico BB84	En los principios de la física cuántica: el principio de incertidumbre de Heisenberg y entrelazamiento cuántico de las partículas.	Alta

Fuente: Revisión bibliográfica
Elaborado por: Mantilla Carmen, 2017

4.4.3 Índice origen de la clave

Un parámetro determinante en la seguridad de la obtención de la clave es que esta sea totalmente secreta y al generarse con software utiliza un algoritmo computacional por lo tanto, la clave de los algoritmos clásicos son determinístico o pseudo aleatorios al tiempo con el avance tecnológico existirán equipos de cómputo capaz de resolver este problema computacional, en contraste con los algoritmos cuánticos que a pesar de no existir la computadora cuántica que a nivel software pueda generar una clave no determinístico se lo realiza a nivel de hardware gracias a las bondades de la física cuántica, siendo cien por ciento aleatoria.

De tal manera que al código speudo aleatorio de la clave generada por el algoritmo RSA se da una valoración media alta con respecto al código aleatorio generado por BB84. Los resultados obtenidos del índice se presentan en la tabla 15-4.

Tabla 15-4 Índice origen de la clave

Nombre del algoritmo	Origen de la clave	Valoración cualitativa
Algoritmo criptográfico clásico RSA	Pseudo aleatoria	Media alta
Algoritmo criptográfico Cuántico BB84	Aleatoria	Alta

Fuente: Revisión bibliográfica
Elaborado por: Mantilla Carmen, 2017

4.4.4 Índice tamaño de la clave

Algo predomínate en los algoritmos clásicos es que es un número determinado el tamaño de la clave por lo que el atacante al interceptar la información, sabrá si obtuvo la totalidad de la clave, al mismo tiempo, mientras más grande la clave tomara más tiempo en descifrar y es más difícil el problema computacional. A diferencia en los algoritmos cuánticos el tamaño de la clave es un número grande que no sigue un patrón por lo que el atacante no sabrá si obtuvo la totalidad de la clave.

Por lo expuesto se considera una valoración media para el algoritmo clásico RSA y alta para el algoritmo cuántico BB84. En la tabla 16-4, se presentan los resultados del análisis con respecto a este índice.

Tabla 16-4 Índice tamaño de la clave

Nombre del algoritmo	Tamaño de la clave	Valoración cualitativa
Algoritmo criptográfico clásico RSA	Tamaño de clave mayor o igual a 1024 bits	Media
Algoritmo criptográfico Cuántico BB84	N	Alta

Fuente: Revisión bibliográfica
Elaborado por: Mantilla Carmen, 2017

4.4.5 Índice el atacante copia la información

Sin duda una de las fortalezas de la criptografía cuántica frente a la clásica es el principio de incertidumbre de Heisenberg que nos dice que no se pueden copiar un estado de una partícula ya que al medirlo se perturba el sistema lo que produce que esta interferencia dañe la información, a diferencia de la criptografía clásica en un ataque de intercepción se puede adquirir en su totalidad la clave. Por lo que se ha dado una valoración alta a él algoritmo cuántico y bajo a él algoritmo clásico. Se presentan los resultados del estudio de este índice en la tabla 17-4.

Tabla 17-4 Índice el atacante copia la información

Nombre del algoritmo	El atacante copia la información	Valoración cualitativa
Algoritmo criptográfico clásico RSA	SI	Baja
Algoritmo criptográfico cuántico BB84	NO	Alta

Fuente: Revisión bibliográfica
Elaborado por: Mantilla Carmen, 2017

4.4.6 Índice detección de intrusos

El principio de incertidumbre de Heisenberg nos dice que al existir perturbación en el sistema podemos determinar que se hizo un intento de medir l información del canal cuántico lo que delata al intruso, en la criptografía clásica no hay manera de determinar si existe un intruso en la comunicación cuando ha burlado todos los filtros de seguridad. Por lo cual da una valoración baja al algoritmo clásico y una alta al algoritmo cuántico. Los resultados de dicho análisis de muestran en la tabla 18-4.

Tabla 18-4 Índice detección de intrusos

Nombre del algoritmo	Detección de intrusos	Valoración cualitativa
Algoritmo criptográfico clásico RSA	**NO** detecta si un atacante escucha el canal.	Baja
Algoritmo criptográfico cuántico BB84	**SI** detecta si un atacante escucha el canal.	Alta

Fuente: Revisión bibliográfica
Elaborado por: Mantilla Carmen, 2017

4.4.7 Índice tecnología aplicada en el mercado

Algo importante a considerar es la implementación y utilización de las tecnologías de la criptografía en el medio comercial ya que RSA se utiliza en diferentes dispositivos comercializados para transmisión de la información ya que ha pasado a producción y desarrollo en cambio la criptografía cuántica es una tecnología emergente y de experimentación que a la vez no se ha desarrollado en su totalidad y tiene sus limitaciones. Por este motivo se le atribuye una valoración media baja a la criptografía cuántica y a la criptografía clásica una valoración alta. En la tabla 19-4, se muestran los resultados del índice estudiado.

Tabla 19-4 Índice tecnología aplicada en el mercado

Nombre del algoritmo	Tecnología aplicada en el mercado	Valoración cualitativa
Algoritmo criptográfico clásico RSA	Comercial y muy utilizada en producción	Alta
Algoritmo criptográfico Cuántico BB84	Poco comercial, tecnología en desarrollo mantiene limitaciones	Media baja

Fuente: Revisión bibliográfica
Elaborado por: Mantilla Carmen, 2017

4.4.8 Resumen comparativo de los parámetros para comparación de los algoritmos clásicos y cuánticos

En tabla 20-4, se presenta un resumen de los índices considerados para la comparación entre algoritmos criptográficos clásico RSA y cuántico BB84.

Tabla 20-4 Resumen de parámetros comparativos de algoritmos criptográficos clásicos vs cuánticos

Algoritmo	RSA	BB84
Unidad estructural de información	Media	Alta
Base de la seguridad	Media Alta	Alta
Origen de la clave	Media alta	Alta
Tamaño de la clave	Media	Alta
El atacante copia la información	Baja	Alta
Detección de intrusos	Baja	Alta
Tecnología aplicada	Alta	Media baja

Fuente: Revisión bibliográfica
Elaborado por: Mantilla Carmen, 2017

El gráfico 5-4, representa un resumen de todos los índices que se han considerado para determinar, el algoritmo criptográfico que se ajusta en mejor medida para la seguridad en la obtención de la clave considerando como representativo del grupo de los clásicos RSA

y de los cuánticos BB84. Como se puede observar los valores más altos se centran en BB84.

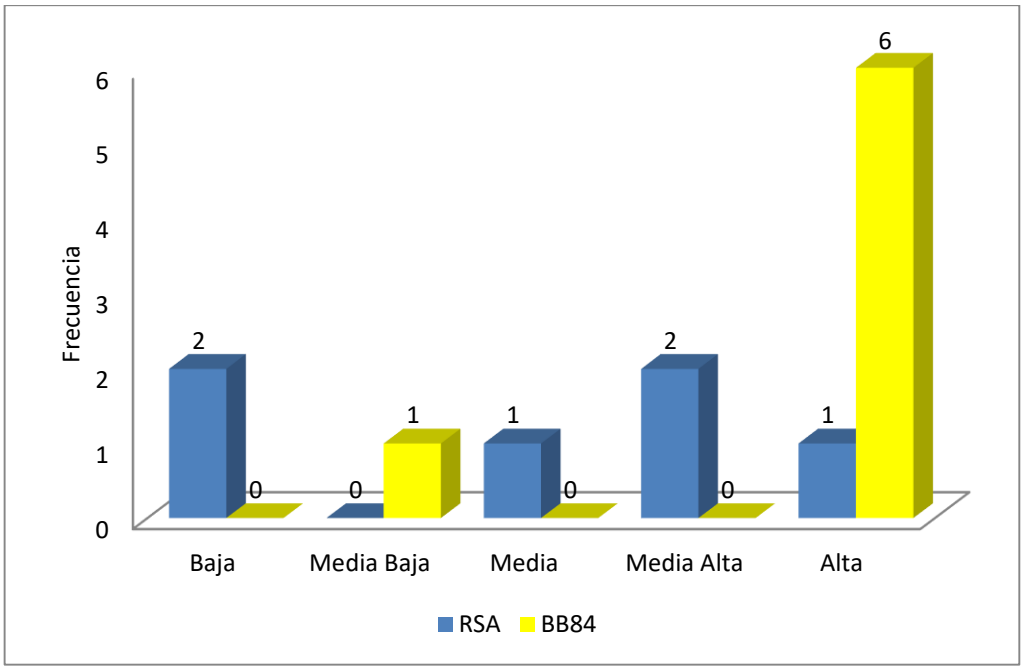

Gráfico 5-4 Valoración cualitativa índices comparativos RSA y BB84

Fuente: Análisis de índices
Elaborado por: Mantilla Carmen, 2017

4.4.9 Comprobación de la Hipótesis General

Para la comprobación de la Hipótesis General los algoritmos criptográficos cuánticos son más adecuados que los clásicos en la seguridad de la obtención de clave, se utilizó la estadística no paramétrica el estadístico Chi Cuadrado, con los resultados obtenidos de los índices comparativos de los algoritmos tanto clásicos como cuánticos

1.- Se determinó la siguiente hipótesis nula H_o y la Alternativa H_1 que son:

Hipótesis Nula H_0: Los algoritmos cuánticos son igual de apropiados que los clásicos para la seguridad en la obtención de clave.

Hipótesis de investigación H_1: Los algoritmos cuánticos son más apropiados que los clásicos para la seguridad en la obtención de clave.

La representación estadística de la hipótesis nula y la alternativa sería:

$$H_0: \mu_{clásicos} = \mu_{cuánticos}$$
$$H_1: \mu_{cuánticos} > \mu_{clásicos}$$

La hipótesis Nula (H_o) Los algoritmos criptográficos cuánticos son igual de adecuados que los clásicos en la seguridad de obtención de datos, con un nivel de significancia del 5% en la prueba de chi cuadrado X^2.

La hipótesis Alternativa de investigación (H_1) Los algoritmos criptográficos cuánticos son más adecuados que los clásicos en la seguridad de la obtención de clave.

2.- Con un nivel de significancia del 5% en la prueba de chi cuadrado X^2.

α=5 %=0.05

3.- Para comprobar la hipótesis se utilizó la tabla de resultados de comparación de los índices entre el algoritmo criptográfico cuántico BB84 y el clásico RSA. Donde se obtuvo los siguientes resultados preliminares que consideramos como valores Observados, como se muestra en la tabla 21-4 y los valores esperados en la tabla 22-4.

Tabla 21-4 Valores observados

Valores Observados			
Valoración	**RSA**	**BB84**	**Total**
Baja	2	0	2
Media Baja	0	1	1
Media	1	0	1
Media Alta	2	0	2
Alta	1	6	7
TOTAL	**6**	**7**	**13**

Fuente: Tabla de contingencia índices de comparación
Elaborado por: Mantilla Carmen, 2017

Tabla 22-4 Valores esperados

Valores Esperados			
Valoración	**RSA**	**BB84**	**Total**
Baja	0.92	1.08	2
Media Baja	0.46	0.54	1
Media	0.46	0.54	1
Media Alta	0.92	1.08	2
Alta	3.24	3.76	7
TOTAL	**6**	**7**	**13**

Fuente: Calculo valores esperados
Elaborado por: Mantilla Carmen, 2017

Obtenidos los Valores Esperados se determinar el valor de X^2 prueba Chi cuadrado con la ecuación 4.1:

$$X^2 = \sum_{i=1}^{r} \sum_{j=1}^{k} \frac{(O_{ij} - E_{ij})^2}{E_{ij}} \quad (4.1)$$

Dónde:

Oij, frecuencias observadas (número de casos observados clasificados en la fila i de la columna j).

Eij, frecuencias esperadas (número de casos esperados correspondientes a cada fila y columna).

Aplicando la ecuación 4.2, obtenemos:

$$X^2 = \frac{(O_{11} - E_{11})^2}{E_{11}} + \frac{(O_{22} - E_{22})^2}{E_{22}} + \cdots \frac{(O_{rk} - E_{rk})^2}{E_{rk}} \quad (4.2)$$

$$\boldsymbol{X^2 calculado = 9.60}. \text{ Calculado.}$$

4.- Se determinó el valor de chi cuadrado de la Tabla X^2 tabla para lo cual se necesita los grados de libertad (gl) y el nivel de significancia que es del 5%, gl se expresa en la ecuación (4.3).

$$gl = (r - 1) * (k - 1) \quad (4.3)$$

Donde:

r= N° de columnas

k= N° de filas para este caso tenemos:

$$gl = (2 - 1) * (5 - 1)$$

$$gl = 4$$

El valor crítico indicado en la tabla de chi - cuadrado en el Anexo B es:

$\boldsymbol{X^2crítico = 9.488,}$ que se representa en el grafico 6-4.

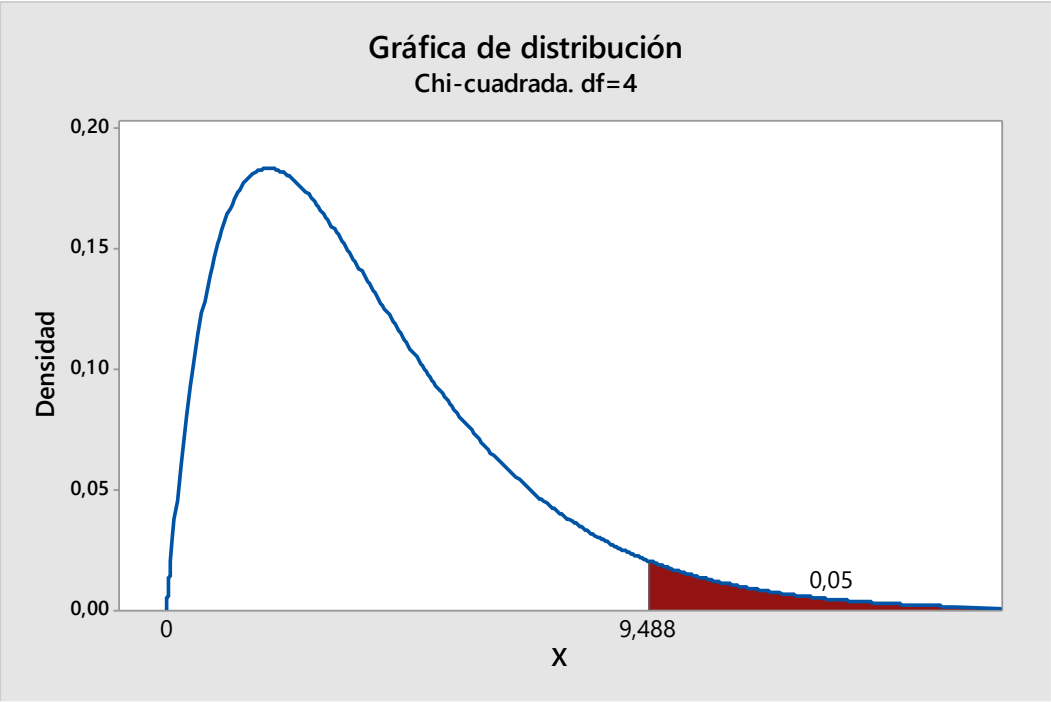

Gráfico 6-4 Grafica de región de rechazo y región de aceptación

Fuente: SPSS
Elaborado por: Mantilla Carmen, 2017

Puesto que$X^2 calculado = 9.60 > X^2 crítico = 9.448$ Se rechaza Hoy se acepta H1

De acuerdo a los datos obtenidos el X^2 de la tabulado y X^2 calculado se concluye que se rechaza la hipótesis nula y se acepta la hipótesis alternativa, los algoritmos criptográficos cuánticos son más apropiados que los clásicos en la seguridad en la obtención de clave, con un nivel de significancia del 5% en la prueba de chi cuadrado X^2.

La comprobación de la hipótesis por el método del X^2 permite identificar que los algoritmos criptográficos cuánticos son más apropiados en la seguridad en la obtención de clave.

DISCUSIÓN

La aplicabilidad y versatilidad de RSA a la hora de brindar seguridad en la obtención de clave radica en la fortaleza de su algoritmo de factorización, pero las claves generadas al ser speudo aleatorias con el tiempo y los avances tecnológicos lograran resolver estos problemas computacionales, lo que no sucede con las claves cuánticos que son verdaderamente aleatorios (Benet, 2015; Saudi, 1998).

Ekert, menciona que teóricamente el algoritmo de entrelazamiento cuántico E91, es el más seguro para la seguridad de distribución de claves, pero es necesario recalcar que este algoritmo es relativamente nuevo y según los índices de estudio tiene limitaciones para su implementación, ya que su aplicabilidad se ve limitada por dispositivos desarrollados que todavía se encuentran en fase experimental. (Ekert, 1991)

Benet destaca que E92 es una mejora de algoritmo BB84, que es más rápido, que tiene ventajas en el proceso de reconciliación de claves sin embargo al compararlo con BB84 (Bennett, 1992), esta misma fortaleza indica que en este proceso se pierden información por lo que, si esto sucede es necesario volver a generar la clave, al mismo tiempo BB84 es un algoritmo en fase de producción, brindando confiabilidad a las empresas que lo implementen (Bennett, Bessette, Brassard, Salvail & Smolin, 1992).

CAPITULO V

5. PROPUESTA

Tomando como base fundamental el estudio realizado de la comparación de los algoritmos clásicos vs cuánticos, se detallan la propuesta como solución para la implementación de un sistema cuántico en la infraestructura gubernamental CNE de Ecuador, se da las conclusiones y recomendaciones del presente trabajo.

5.1. Exposición de la propuesta para la implementación de un sistema cuántico con BB84

En este capítulo se refleja el producto de la investigación, que propone un estudio comparativo para destacar las ventajas en la seguridad de obtención de clave de los algoritmos criptográficos cuánticos sobre los clásicos sustentado teóricamente y matemáticamente en una revisión sistemática, al determinar que el algoritmo criptográfico cuántico BB84 es el más adecuados para la seguridad en la obtención de clave, se presenta una propuesta la implementación de esta tecnología para estructura del Consejo Nacional Electoral (CNE) nacional actual, determinando el equipamiento técnico y los costos. Esta estructura centralizada en la capital ecuatoriana permitiría realizar el sufragio encriptado a tiempo real y conteo desde las delegaciones sucursales en las provincias.

5.2. Análisis de requerimientos técnicos para implementación de BB84

En este apartado se presenta el estudio de requerimientos técnicos necesarios para la implementación del sistema criptográfico cuántico BB84.

En el grafico 1-5 se mostró cómo funciona la comunicación cuántica a manera de bloques, la forma como puede coexistir la criptografía clásica con la cuántica para que se pueda

usar en las aplicaciones comunes para la comunicación. Ahora es necesario desglosar cada bloque y mostrar en forma más específica las partes que constituyen, el gráfico 2-5, muestra este sistema de manera que se puede realizar la transmisión de la clave en forma segura, utilizando el algoritmo criptográfico BB84 para la distribución de la clave.

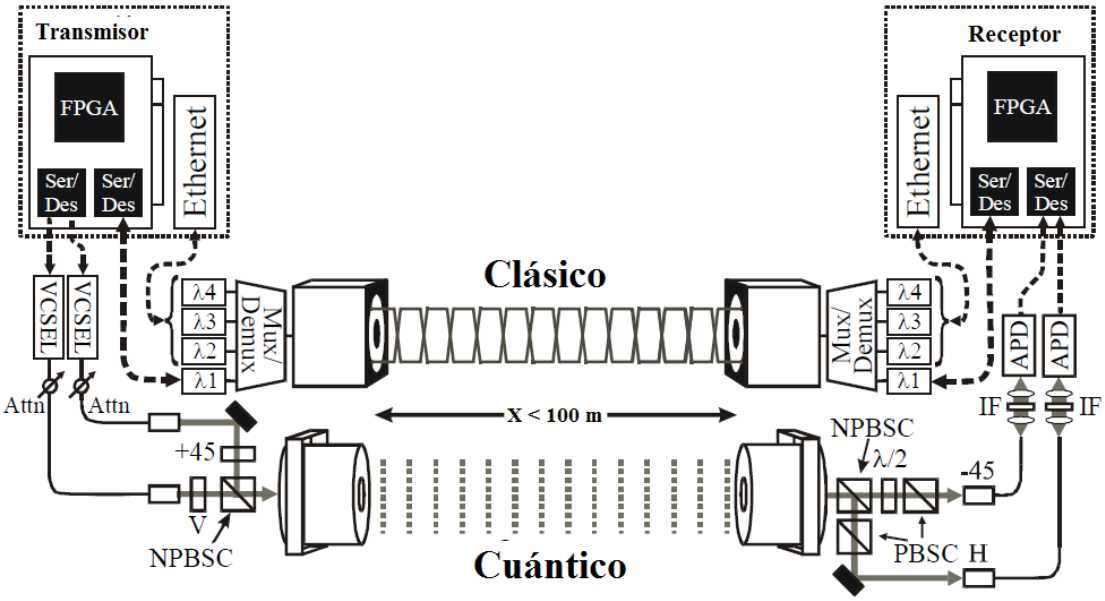

Gráfico 7-5 Esquema para comunicación cuántica

Fuente: (Chuang, 2000)
Elaborado por: Mantilla Carmen, 2017

En la tabla 1-5, se presentan las componentes de este sistema, los requerimientos tecnológicos que son necesarios para la implementación del algoritmo criptográfico para la distribución de clave BB84, para que pueda trabajar en un sistema clásico.

Tabla 1-5 Requerimientos técnicos para la implementación de BB84

Requerimiento	Descripción
Canal clásico	Internet dedicado
Canal cuántico	Enlace de fibra óptica de 845nm.
Ethernet	Gigabit Ethernet
PCI	Tarjeta PCI
Attn	Atenuadores
NPBSP	Cristal de divisor de haz de luz no polarizado.

PBSC	Cristal de divisor de haz de luz polarizado.
VCSEL	Fuente láser para emisión de superficie de cavidad vertical de 10 GHz.
IF	Filtro espectral
APD	Fotodiodo avalancha
FPGA	Arreglo de compuertas programable por campo
Multiplexor	Multiplexor divisor de onda ancha (WDM), con cuatro canales full dúplex de canales a 1.25 Gbps.

Fuente: (Chuang, 2000)
Elaborado por: Mantilla Carmen, 2017

5.3. Equipamiento

En los gráficos 3-5,4-5, 5-5, 6-5, 7-5, se presentan los equipos que cumplen con las funciones para los requerimientos técnicos para la implementación.

Gráfico 8-5 Generador de números aleatorios para aplicaciones de red

Fuente: http://www.idquantique.com/quantum-safe-crypto/quantis-rng-appliance

Características:

- Aleatoriedad cuántica cierto, con NGRQ interno certificado.
- Conexión en caliente y swappable en redes de explotación.
- Comprobación del estado de ejecución y el reinicio automático en caso de anomalías
- Alta tasa de bits de hasta 16 Mbits / s,
- Sistema de montaje en rack: estándar "1U 19

Gráfico 9-5 Tarjeta PCI

Fuente: www.becker-hickl.com

Características:

- Entrada con discriminador de ancho de banda de 4 GHz
- Sub-ps oscilación de tiempo de baja frecuencia
- Capacidad Multi-detector / multi-longitud de onda
- Distribución de fotones y modos parámetros-etiquetados
- FLIM por bh tecnología en Megapixel.
- Modo mosaico FLIM
- Modo multi escalar
- Intensidades para FLIM canal contador paralelo
- Operación paralela de 2, 3 o 4 módulos
- Tiempo de canal bajo 813 fs
- Tiempo de resolución eléctrica (Jitter) 2.5 psrms
- Rata de repetición laser sobre 150 MHz
- Rata de saturación de contador de 12.5 MHz
- TCSPC final tiempo 80 ns
- Intensidad de muerte de canal tiempo <10 ns

Gráfico 10-5 Atenuador

Fuente: http://www.becker-hickl.com/amplifiers.htm#hfah

Características:

- Convertidor de frecuencia análoga para pulsos PMT.
- Entrada de pulso de amplitud de -30 mV a-200 mV
- Ancho de entrada de pulso bajo 500 ps
- Línea de pulso en detector para insertar directamente
- Compatibilidad con módulos bh PMT y detectores híbridos.
- Rata de pulsos de entrada a 10^7 pulsos por segundo
- Rango de salida de voltaje 0 a +4.9 V
- Alimentación ± 5V desde módulos bh SPC o DCC

Gráfico 11-5 Servidor de QKD

Fuente: http://www.idquantique.com/quantum-safe-crypto/qkd-server/

Características:

- Proporciona un intercambio de claves cuántico-seguro: robusto contra ataques de computadoras cuánticas
- Seguridad a prueba de futuro: las claves cuánticas garantizan la protección de datos a largo plazo y el secreto hacia adelante
- Integrado con los cifradores de enlace Centauris y ampliamente desplegado en el mercado desde 2007
- Versátil: puede proporcionar claves cuánticas seguras para cualquier dispositivo de cifrado
- Escalable: un servidor de clave cuántica puede distribuir claves a varios cifradores para un máximo de 100 Gbps de datos
- Intercambio de llaves completamente automatizado con renovación continua de llaves

- Fuente de entropía integrada basada en un generador de números aleatorios cuánticos
- Adaptable: Funciona en redes de fibra oscura y WDM

Gráfico 12-5 Cliente de QKD

Fuente: http://www.idquantique.com/quantum-safe-crypto/qkd-blade-server/

Características:

- Probabilidad de intercambio de claves seguro basado en QKD: robusto contra ataques de ordenadores cuánticos
- Seguridad a prueba de futuro: las claves cuánticas garantizan la protección a largo plazo y el secreto hacia adelante
- Intercambio de llaves completamente automatizado con renovación continua de llaves
- Fuente de entropía integrada basada en un generador de números aleatorios cuánticos
- Compatible con KMIP para máxima versatilidad
- Diseño resistente a manipulaciones

5.4. Propuesta de implementación de criptografía cuántica BB84 en la infraestructura gubernamental Consejo Nacional Electoral (CNE) de Ecuador

El Consejo Nacional Electoral de Ecuador es una de los organismos gubernamentales que maneja información sensible, debido a que cada periodo de cuatro años se realizan las elecciones electorales presidenciales, en la actualidad en las recientes elecciones se escucharon murmuraciones que no se han comprobado alegando que ha existido fraude electoral, en las que hackers han sustituidos los resultados de las actas.

En Ecuador como un país subdesarrollado los sistemas computacionales para este propósito cuentas con seguridades convencionales, la propuesta que se presenta, es la implementación de una estructura centralizada para sufragar, que se compone de una central de votaciones en la capital del país, Quito y sus 22 sucursales distribuidas a nivel en cada provincia, el gráfico 8-5, muestra la localización geográfica de la estructura actual de CNE que se va a implementar en una estructura estrella, donde icono amarillo representa la Central y los rojos las delegaciones sucursales.

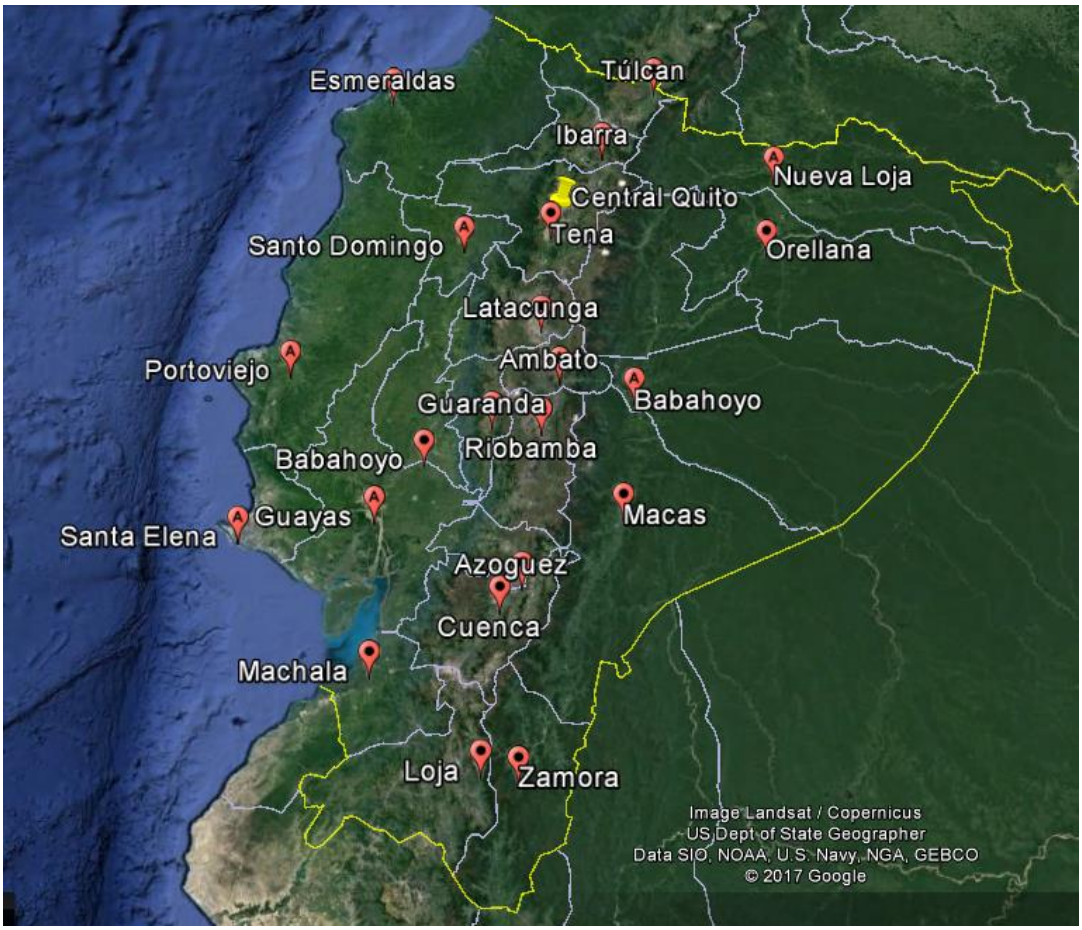

Gráfico 13-5 Ubicación geográfica de la estructura a implementar
Fuente: Google Earth

Para determinar las distancias que se debe cubrir en la implementación se ha considerado las delegaciones continentales, por lo que no consta Galápagos debido a que se deben realizar instalaciones subterráneas y se deben estimar otros valores, la tabla 3-5, muestra la distancia de cada delegación en las provincias con una distancia lineal estimada hacia la Central Quito.

Tabla 2-5 Ubicación actual de las delegaciones existentes de CNE

Delegación	Ubicación	Distancia(Km)
Azuay	Calle Tarqui 1158 Y Sangurima (Cuenca)	305
Bolívar	Calle Azuay 509 E/ Sucre Y Convención 1884 (Guaranda)	168
Cañar	Calle Alberto Sarmiento Y David Mogrovejo (Azogues)	285
Carchi	Av. Coral Y Venezuela N° 59060 (Tulcán)	138
Chimborazo	Calle Colon 25-18 Y Orozco (Riobamba)	158
Cotopaxi	Calle General Proaño Y Sánchez De Orellana (Latacunga)	80
El Oro	Calle Rocafuerte 1301 Y Santa Rosa (Machala)	378
Esmeraldas	Av. Eloy Alfaro Y Manuela Cañizares (Esmeraldas)	183
Galápagos	Av. Alsacio Northia Y Hernán Merville (Puerto Baquerizo Moreno Isla San Cristóbal)	-
Guayas	Av. Democracia Y Roberto Gilbert	272
Imbabura	Av. Jaime Roldos 1-165 Y Sánchez Y Cifuentes (Ibarra)	83
Loja	Calle Bernardo Valdiviezo E/ 10 De Agosto Y Rocafuerte (Loja)	434
Los Ríos	Cdla El Mamey Av. Universitaria Y Calle 1-Ne (Babahoyo)	210
Manabí	Calle 15 De Abril Y Teodoro Wolf (Portoviejo)	240
Morona Santiago	Calle Manuel Moncayo Y 24 De Mayo (Macas)	237
Napo	Av. Las Palmas Y Manuela Cañizares N° 110 (Tena)	6
Orellana	Calle Amazonas Y Juan Montalvo (Francisco De Orellana)	172
Pastaza	Av. Alberto Zambrano Palacios S/N Y Rio Tigres (Puyo)	161
Pichincha	Calle Iñaquito N° 35-227 E Ignacio San María (Quito)	-
Santa Elena	Barrio Los Amantes De Sumpa (Santa Elena)	347
Sto. Dgo. Tsachilas	Calle Julio Cesar Bermeo Detrás Del Terminal Terrestre (Santo Domingo)	75
Sucumbíos	Calle Venezuela 1301 Y 20 De Junio (Nueva Loja)	185
Tungurahua	Gustavo Adolfo Becker Y Azorín (Ambato)	121
Zamora Chinchipe	Calle José Duran Y Flavio Paz (Zamora)	429
	Total Km.	**4467**

Fuente: CNE
Elaborado por: Mantilla Carmen, 2017

Como se puede observar la distancia mínima es de 6 Km hacia la sucursal Tena, la máxima de 434 Km hacia la de Loja, la distancia promedio aproximada es de 212 Km y un total de 4467 Km que se deben considerar para la implementación de la estructura.

5.5. Empresas de soluciones tecnológicas cuánticas

Existen varias empresas en el mercado con productos para varias aplicaciones de mecánica cuántica, las empresas que se presentan proveen de varios productos para criptografía cuántica en producción.

IDQ.- es una de las empresas que ha recibido varios premios internacionales líder a nivel mundial en tecnologías de la física cuántica, proporciona soluciones de criptografía cuántica y conocimientos que permiten a sus clientes a resolver problemas mediante la explotación del potencial de la física cuántica.

Ofrece cifradores cuánticos de hasta 100 Gbps en redes de área local y de almacenamiento para centro de datos de interconexión y la RDC, contadores de fotones soluciones innovadoras para aplicaciones industriales, comerciales y de investigación, estos contadores de fotones pueden ser de región visible o infrarroja de espectro óptico, las fuentes de láser de pulso corto, plataformas de QKD para aplicaciones de investigación y desarrollo y Generadores de números aleatorios (NGRQ) basados en la física cuántica, que se utilizan en varias industrias en la seguridad, juegos y sorteos.

Boston Electrónica.- es una empresa Suiza fabricante especialista productos para criptografía cuántica ofrece soluciones en fotodetección y generación de fotones con sus productos para recuento de fotones individuales sistemas y componentes, detectores UV o IR y fuentes de luz, y los láseres IR sintonizable.

becker-hickl.- Becker & Hickl han introducido un principio patentado de contaje de un solo fotón basado en el tiempo que hizo TCSPC más rápido que los dispositivos existentes. Ofrece productos TCSPC bh que se complementan con láser de diodo de pico segundos, bh, módulos de detectores, conjuntos de detectores multi espectrales y módulos de control de experimentos, microscopio confocal de exploración láser de fluorescencia y kits de actualización FLIM para microscopios de escaneo láser de varios fabricantes.

5.6. Análisis económico

En la Tabla 2-5, se presenta los valores económicos necesarios para la implementación de un sistema de encriptación cuántica con BB84 para un máximo de 100Km.

Cerberis QDK Server es una versión versátil para la solución de implementación de una empresa, incluye el servicio por un año de canal de fibra óptica, el software necesario para que se realice la transmisión de claves, además de las actualizaciones y garantías sobre equipos y servicios para el normal desempeño del sistema.

Tabla 3-5 Requerimientos económicos para la implementación de BB84

Equipo	Costo ($)
Cerberis QKD Server (Emisor) – 12/4 puertos	47000
Cerberis QKD Server (Receptor) – 12/4 puertos	47000
Licencia para puertos para dispositivos Cerberis (máximo. 12 puertos)	3500
Servicio de fibra óptica para canal cuántico	
Software	53500
Servicio y soporte para un año	
Actualizaciones	
Garantía	
TOTAL	**150.000**

Fuente: Proforma IDQ
Elaborado por: Mantilla Carmen, 2017

Según el Ministerio de Finanza el presupuesto anual para el año 2017 es de casi $ 37 mil millones de dólares para gasto público, dando prioridad a la educación, por lo que la propuesta presenta una estimación económica de la implementación de criptografía cuántica con BB84 para la seguridad de la infraestructura de CNE nacional, con miras a generar interés para la inversión y comparaciones de costo beneficio en la seguridad de la información de este estamento gubernamental.

El total de la distancia a instalar es aproximadamente 4467 Km., con un costo de $ 150.000 por cada 100 Km., por lo que se estima alrededor de $ 7.700.550 del valor total para implementar criptografía cuántica en CNE, considerando el 10% de imprevistos (Shapiro, 2007).

CONCLUSIONES

- De la revisión bibliográfica sistemática se determinó que los algoritmos RSA y BB84 son los más fuertes para la seguridad de la obtención de clave de los algoritmos criptográficos clásicos y cuánticos respectivamente.

- Se estableció siete índices de evaluación para la comparación de algoritmos clásicos y cuánticos que son: unidad estructural de la información, base de su seguridad, origen de la clave, tamaño de la clave, si el atacante copia la información, detección de intrusos y tecnología aplicada en el mercado que son variables que se utilizan para determinar la fortaleza de los algoritmos en la seguridad en la obtención de la clave.

- Al aplicar el método estadístico CHI CUADRADO se obtuvo un valor de 9.488, concluyéndose que el algoritmo criptográfico BB84 es el más adecuado para la seguridad en obtención de claves, por lo que se induce que los algoritmos criptográficos cuánticos son más apropiados para la seguridad en la obtención de clave.

- La propuesta de implementación de criptografía cuántica en la infraestructura nacional de CNE de 22 delegaciones continentales, es técnicamente factible y su costo representa el 0.022% del presupuesto anual del gasto público 2017, mejorando la seguridad en su información

- Este estudio se enmarca en el objetivo 11.3 del Plan Nacional del Buen Vivir, aportando con conocimiento para la seguridad de la información gubernamental sensible, representa una base referencial para la fase de implementación futura de esta tecnología en Ecuador.

RECOMENDACIONES

- Debido a que al momento solo es posible generar claves a nivel hardware, se recomienda desarrollar software que permita la simulación del proceso de generación de claves cuánticas y evaluar su comportamiento en un sistema de transmisión.

- Se recomienda realizar un seguimiento continuo a la investigación de los algoritmos criptográficos cuánticos relacionados con la seguridad en la obtención de clave, para la actualización de los resultados de la presente investigación.

- Previo a la implementación de la propuesta se recomienda realizar una fase de implementación experimental que corrobore los resultados analíticos obtenidos y un estudio técnico-económico individualizado para cada sucursal que contemple la orografía del sector y sus particularidades.

- Se recomienda implementar la propuesta técnica económica planteada en la presente investigación para la infraestructura de CNE en función de garantizar la seguridad de la información.

- Se recomienda crear grupos de criptografía cuántica para la seguridad de la información en la ESPOCH con profesionales de diversos perfiles que contribuyan en la temática, esto aportaría para que se implemente este tipo de tecnologías en el país, debido a que en Ecuador no se están realizando estos estudios, posicionando a nuestra universidad como pionera en investigaciones innovadores y de utilidad para la seguridad telemática.

BIBLIOGRAFIA

Alexi, W. & Chor, B. (1988). *RSA and Rabin functions:certeins parts are hard as the whole.* Recuperado 28 de febrero de 2017, a partir de http://www.wisdom.weizmann.ac.il/~oded/X/acgs.pdf

Alayont, F. (2003). *Cryptograph y and Cryptanalysis*. Recuperado 1 de marzo de 2017, a partir de http://faculty.gvsu.edu/alayontf/talks/crypto.pdf

Bautista, L. (2015). *Fenómenos ondulatorios de la luz*. Recuperado 11 de mayo de 2015, a partir de http://www.fisicanet.com.ar/fisica/ondas/ap11_luz.php

Beckman, B. (2002). *Codebreakers. Arne Beurling and the Swedish Crypto Program during World War II.* Recuperado 28 de febrero de 2017, a partir de https://mediatum.ub.tum.de/doc/1323891/1323891.pdf

Boneh, D. (1998). *The Decision Diffie-Hellman problem. En J. P. Buhler (Ed.), Algorithmic Number Theory* (pp. 48-63). SpringerBerlin Heidelberg. Recuperado a partir de http://link.springer.com/chapter/10.1007/BFb0054851

Bennett, C., Bessette, F., Brassard, G., Salvail, L., & Smolin, J. (1992). *Experimental* quantum cryptography. *Journal of Cryptology*, *5*(1), 3-28. https://doi.org/10.1007/BF00191318

Bennett, C. (1992, mayo 25). *Quantum Cryptography Using Any Two Nonorthogonal States.* Recuperado 31 de julio de 2015, a partir de http://www.infoamerica.org/documentos_pdf/bennett1.pdf

Benet, M. (2015). *Criptografía en clave pública y privada. RSA*. Recuperado 28 de febrero de 2017, a partir de http://repositori.uji.es/xmlui/bitstream/handle/10234/139037/TFG_2015_EcobarBenetM.pdf;jsessionid=AF67959A7ACADFFB1AFD5F405766B50E?sequence=1

Beth, Th. (1992). *Public-Key Cryptography: State of the Art and Future Directions : E.I.S.S.* Workshop, Oberwolfach, Germany.

Born, M. (1968). *Physics in My Generation*. Recuperado 13 de mayo de 2015, a partir de http://www.google.com.ec/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&cad=rja&uact=8&ved=0CCcQFjAB&url=http%3A%2F%2Fwww.springer.com%2Fcda%2Fcontent%2Fdocument%2FproductFlyer%2FproductFlyer_978-1-4615-7587-0.pdf%3FSGWID%3D0-0-1297-174949966-0&ei=B8lSVe6lCsi-ggTU9YDQCg&usg=AFQjCNEhn-VJehZ0Zleypja4_8n-88Gy1g&bvm=bv.93112503,d.eXY

Botaya, J. (2005). *Universitat Oberta de Catalunya.* Obtenido de http://openaccess.uoc.edu/webapps/o2/bitstream/10609/674/1/34993tfc.pdf

Caesar. J. (2013). *Cryptography*. Recuperado 1 de marzo de 2017, a partir de https://www.cl.cam.ac.uk/~rja14/Papers/SE-05.pdf

Calude C., & Svozil, K. (2006). *Quantum Randomness and Value Indefiniteness.* Recuperado 13 de mayo de 2015, a partir de https://www.cs.auckland.ac.nz/research/groups/CDMTCS/researchreports/291cris.pdf

Chuang, I. (2000). *Quantum algorithm for distributed clock synchronization*. Recuperado 1 de marzo de 2017, a partir de https://arxiv.org/pdf/quant-ph/0005092.pdf

Churchhouse, R. (2014). *Code and ciphers: Julius Caesar, the Enigma and the internet*. Recuperado a partir de http://www.ik4hdq.net/codici_cifr.pdf

Ciencia, P. (2006). *Física Cuántica.* Recuperado 11 de mayo de 2015, a partir de http://www.cienciapopular.com/ciencia/fisica-cuantica

Cochen, S., & Specker, E. (1969). *The Problem of Hidden Variables in Quantum Mechanics.* Recuperado 13 de mayo de 2015, a partir de http://link.springer.com/chapter/10.1007/978-3-0348-9259-9_21#page-1

Cook. S. (1983). *An overview of computational complexity*. Recuperado 3 de agosto de 2015, a partir de http://www.jdl.ac.cn/turing/pdf/p400-cook.pdf

Corrales, H., Cilleruelo, C. & Cuevas A. (2011). *Criptografía y Métodos de Cifrado*. Recuperado 27 de julio de 2015, a partir de http://www2.uah.es/libretics/concurso2014/files2014/Trabajos/Criptograf%EDa%20y%20M%E9todos%20de%20Cifrado.pdf

Daemen, J. & Rijmen, V. (2001, noviembre 26). AES - *The Advanced Encryption Standard*. Recuperado 31 de julio de 2015, a partir de http://jda.noekeon.org/JDA_VRI_Rijndael_2002.pdf

Delgado, L., & Vallejo, R. (2009). *Universidad de Nariño.* Obtenido de http://sired.udenar.edu.co/288/1/Curvas%20El%C3%ADpticas%20Construidas%20sobre%20Campos%20Finito%20y%20Criptograf%C3%ADa.pdf

Donado, S., Niño, M. & Flechas, F. (2001). *Seguridad Computacional* Rev2. Recuperado 27 de julio de 2015, a partir de https://es.scribd.com/doc/209937456/2001-05-15-Seguridad-Computacional-Rev2

Ekert, A. (1991). *Quantum cryptography based on Bell's theorem*. *Physical Review Letters, 67*(6), 661-663. https://doi.org/10.1103/PhysRevLett.67.661

ElGamal, T. (1985). *A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms. En G. R. Blakley& D. Chaum (Eds.), Advances in Cryptology* (pp.

10-18). Springer Berlin Heidelberg. Recuperado a partir de http://link.springer.com/chapter/10.1007/3-540-39568-7_2

Fortnow, L. & Homer, S. (2002). *A Short History of Computational Complexity*. Recuperado 3 de agosto de 2015, a partir de http://people.cs.uchicago.edu/~fortnow/papers/history.pdf

Frances, V. (2013). *Propuesta y análisis de criptosistemas de clave pública basados en matrices triangulares superiores por bloques*. Recuperado a partir de https://rua.ua.es/dspace/bitstream/10045/4081/1/tesis_doctoral_vicent_frances.pdf

Galende, C. (1995). *La cirptografía medieval.* Recuperado 1 de marzo de 2017, a partir de http://pendientedemigracion.ucm.es/info/citechar/jornadas/II%20JORNADAS/jor02galende.pdf

Gálvez, N. (2014). *Análisis y mejora del rendimiento del algoritmo aes para su utilización en teléfonos móviles*. Recuperado 28 de febrero de 2017, a partir de http://148.204.210.201/tesis/1404316762511NPGMTesisAn.pdf

García, A., García, F. & García, J. (2014). *Criptografía cuántica*. Recuperado 11 de mayo de 2015, a partir de http://www.criptored.upm.es/crypt4you/temas/cuantica/leccion2/leccion02.html

García, R. (2014). *Polarizadores*. Recuperado 11 de mayo de 2015, a partir de http://www.upv.es/satelite/trabajos/Grupo9_99.00/polarize.htm

Hernández, A. & Reyes, A. (2014). *Metaanálisis del estado actual de la criptografía cuántica identificando las áreas de desarrollo.* Universidad Católica de Colombia, Bogota. Recuperado a partir de http://repository.ucatolica.edu.co/bitstream/10983/1381/1/01%20-%20METAAN%C3%81LISIS%20DEL%20ESTADO%20ACTUAL%20DE%20LA%20%20CRIPTOGRAF%C3%8DA%20CU%C3%81NTICA%20IDENTIFICANDO%20LAS%20%C3%81REAS%20DE%20DESAR.pdf

Herreros, J. (2004). *Cristales Birrefringentes*. Recuperado 11 de mayo de 2015, a partir de ftp://tesis.bbtk.ull.es/ccppytec/cp196.pdf

Kahn, D. (1973). *TheCodeBreakers.* Recuperado 28 de febrero de 2017, a partir de http://mindguruindia.com/wp-content/uploads/2014/06/MP069_The-CodeBreakers.pdf

Landa, A. (2015). *Criptografía: la evolución algorítmica de la seguridad.* Recuperado 27 de julio de 2015, a partir de http://hipertextual.com/2015/03/criptografia-seguridad

Lucena, M. (2009). *Criptografía y Seguridad en Computadores.*

Marc, S. (2014). *Counter-cryptanalysis*. Recuperado 1 de marzo de 2017, a partir de https://marc-stevens.nl/research/papers/C13-S.pdf

Mermin, N. (2002, julio 19). *Qubit*. Recuperado 11 de mayo de 2015, a partir de http://arxiv.org/pdf/quant-ph/0207118v1.pdf

Mogos, G. (2016). *Software implementation of the quantum key distribution protocol with ququarts, International Journal of Information Processing*, ISSN: 09738215, Vol. 9, No. 4.

Mogos, G. (2015). *Quantum Information and Communication* (Segunda). PUBLISHED BY PUBLISHER. Recuperado a partir de BOOK-WEBSITE.COM

Mogos, G. (2015). *Desarrollar una aplicación informática cliente -servidor integrado técnicas de autenticación y de encriptación cuántica*.

Mogos, G. (2016). *Software implementation of the quantum key distribution protocol with ququarts*, International Journal of Information Processing.

Mogos, G., Radu, Gh. (2015). *QKD protocols – software implementations. Bennett-Brassard vs. Bruss, Review of the Air Force Academy*, ISSN 1842-9238; e-ISSN 069-4733, pp. 81-85.

Mogos, G. (2015). *Intercept-Resend attack on quantum key distribution protocols with two, three and four-state systems. Comparative analysis*, The 2nd International Conference on Information Science and Security.ICISS2015, 14-16 December, Seoul, South Korea.

Mogos, G. (2015). *An experimental comparison of Chen et al. and Bruβ quantum key distribution protocols*, 14th RoEduNet Conference: Networking in Education and Research (NER'2015), 24-26 September, Craiova, Romania, ISBN 978-1-4673-8179-6, pp. 39-43.

Mogos, G. (2015). *Quantum Key Distribution protocol with Four-State Systems - software implementation*, The Eleventh International Multi Conference on Information Processing, 21-23 August, Bangalore, India, Procedia Computer Science, pp. 65-72.

Mogos, G. (2015). *Software implementation of Quantum Key Distribution with six-state systems*, The 2015 International Conference on Business and Information, 7-9 July, Macau.

Mogos, G. (2015). *Comparative analysis of Quantum Key Distribution protocols with two, three and four-state systems*, International Conference of Scientific Paper, 28--30 May, Brasov, Romania.

Mogos, G. (2015). *Software implementation of Bechmann-Pasquinucci and Peres protocol for qutrits*, The 2015 International Symposium on Networks, Computers and Communications, 13-15 May, Hammamet, Tunisia, pp. 1-5.

Mogos, G. (2015). *Quantum Key Distribution - QKD Simulation*, Conferencia Indexada (Springer). The 18th Conference on Quantum Information Processing UTS – QIP.

Nielsen, M., & Chuang, I. (2010). *Quantum Computation and Quantum Information: 10th Anniversary Edition*. Cambridge University Press.

Paguay, M. (2015). *Análisis de algoritmos matemáticos de criptografía pública para mejorar el aprendizaje de la materia de criptografía en la carrera de ingeniería en sistemas de la ESPOCH*.

Pérula, R. (2011). *Algoritmos cuánticos en criptografía y distribución de claves en espacio libre*. Recuperado 1 de marzo de 2017, a partir de http://roboticslab.uc3m.es/roboticslab/sites/default/files/Algoritmos%20cu%C3%A1nticos%20en%20criptograf%C3%ADa%20y%20distribuci%C3%B3n%20de%20claves%20en%20espacio%20libre.pdf

Piris, M. (1999). *Física Cuántica*. Recuperado 11 de mayo de 2015, a partir de http://www.ehu.eus/chemistry/theory/mario.piris/files/fisica_cuantica.pdf

Santamaría, J. (2013). *El logaritmo discreto y sus aplicaciones en Criptografía. España*.

Santiango, C. (2006). *Comisión Interamericana de Telecomunicaciones*. Obtenido de http://www.oas.org/en/citel/infocitel/2006/junio/seguridad_e.asp

Saudi, D. (1998). *A Hardware Model of an Expandable RSA Cryptographic System.* Recuperado 1 de marzo de 2017, a partir de https://drive.uqu.edu.sa/_/aagutub/files/_/thesis/MS_Thesis.pdf

Singh, S. (2000). *Los códigos secretos*. Recuperado 28 de febrero de 2017, a partir de http://assets.espapdf.com/b/Simon%20Singh/Los%20codigos%20secretos%20(2355)/Los%20codigos%20secretos%20-%20Simon%20Singh.pdf

Svozil, Karl. (2011). *Quantum value indefiniteness*. Recuperado 13 de mayo de 2015, a partir de http://arxiv.org/pdf/1001.1436.pdf

SvoziL, Karl. (2009). *Three criteria for quantum random number generators based on beam splitters*. Recuperado 13 de mayo de 2015, a partir de https://researchspace.auckland.ac.nz/bitstream/handle/2292/3868/362karl.pdf?sequence=1

Thakur, J. & Kumar, N. (2011). *DES, AES and Blowfish: Symmetric Key Cryptography Algorithms Simulation Based Performance Analysis*. Recuperado 31 de julio de 2015, a partir de http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.366.831&rep=rep1&type=pdf

Textos, Científicos. (2005). C*riptografía Cuántica - Conceptos de Criptografía*. Recuperado 15 de mayo de 2015, a partir de http://www.textoscientificos.com/criptografia/quantica

Verdul, R. (2015). *Introduction to Cryptanalysis: Attacking Stream Ciphers*. Recuperado 1 de marzo de 2017, a partir de http://www.cs.ru.nl/~rverdult/Introduction_to_Cryptanalysis-Attacking_Stream_Ciphers.pdf

Wiesner, S. (1983). *Conjugate coding. ACM SIGACT News*, *15*(1), 78-88. https://doi.org/10.1145/1008908.1008920

ANEXOS

ANEXO A: GLOSARIO

Encriptar.- Significa transformar información legible a legible con una clave como medida de seguridad, en la transmisión de la información y que no sea entendible por aquel que no sea transmisor ni receptor; usando fórmulas matemáticas complejas.(Verdul, 2015)

Criptoanálisis.- Al aplicar a un texto cifrado métodos matemáticos o sea un criptoanálisis se obtiene el texto simple, un algoritmo de cifrado es decodificado cuando el criptoanálisis lo ha descifrado. (Alayont, 2003).

Desencriptar.- Es la práctica contraria a la encriptación, donde se muestra el texto ilegible a legible, con una clave y aplicando fórmulas matemáticas usadas para la encriptación.(Stevens, 2014)

Confusión.-Significa mezclar, permutar la información, mediante cualquier algoritmo para que provocar distracción a la hora de obtener la información de un texto.

Difusión.- Es mantener el texto cifrado en la forma más compleja posible aplicando algoritmos para que no se pueda visualizar la información transmitida.

Autenticación.- Hace referencia a la comprobación de la sí es un usuario confiable de acuerdo a criterios definidos al sistema al que quiere ingresar.

Números Primos.- Los números primos son aquellos que son divisible para uno y para sí mismos aprovechando esto, a criptografía moderna explota este problema de calcular logaritmos discretos supongamos que tenemos un número x y es el resultado del producto de dos factores a, b, estos dos números son primos por lo que no se puede factorizar n

para tener dos factores primos, para calcularlos faltarían recursos computacionales ilimitados a más de tiempo indefinido (Gálvez, 2014).

ANEXO B: TABLA CHI CUADRADO

P = Probabilidad de encontrar un valor mayor o igual que el chi cuadrado tabulado, ν = Grados de Libertad

ν/p	0,001	0,0025	0,005	0,01	0,025	0,05	0,1	0,15	0,2	0,25	0,3	0,35	0,4	0,45	0,5
1	10,8274	9,1404	7,8794	6,6349	5,0239	3,8415	2,7055	2,0722	1,6424	1,3233	1,0742	0,8735	0,7083	0,5707	0,4549
2	13,8150	11,9827	10,5965	9,2104	7,3778	5,9915	4,6052	3,7942	3,2189	2,7726	2,4079	2,0996	1,8326	1,5970	1,3863
3	16,2660	14,3202	12,8381	11,3449	9,3484	7,8147	6,2514	5,3170	4,6416	4,1083	3,6649	3,2831	2,9462	2,6430	2,3660
4	18,4662	16,4238	14,8602	13,2767	11,1433	9,4877	7,7794	6,7449	5,9886	5,3853	4,8784	4,4377	4,0446	3,6871	3,3567
5	20,5147	18,3854	16,7496	15,0863	12,8325	11,0705	9,2363	8,1152	7,2893	6,6257	6,0644	5,5731	5,1319	4,7278	4,3515
6	22,4575	20,2491	18,5475	16,8119	14,4494	12,5916	10,6446	9,4461	8,5581	7,8408	7,2311	6,6948	6,2108	5,7652	5,3481
7	24,3213	22,0402	20,2777	18,4753	16,0128	14,0671	12,0170	10,7479	9,8032	9,0371	8,3834	7,8061	7,2832	6,8000	6,3458
8	26,1239	23,7742	21,9549	20,0902	17,5345	15,5073	13,3616	12,0271	11,0301	10,2189	9,5245	8,9094	8,3505	7,8325	7,3441
9	27,8767	25,4625	23,5893	21,6660	19,0228	16,9190	14,6837	13,2880	12,2421	11,3887	10,6564	10,0060	9,4136	8,8632	8,3428
10	29,5879	27,1119	25,1881	23,2093	20,4832	18,3070	15,9872	14,5339	13,4420	12,5489	11,7807	11,0971	10,4732	9,8922	9,3418
11	31,2635	28,7291	26,7569	24,7250	21,9200	19,6752	17,2750	15,7671	14,6314	13,7007	12,8987	12,1836	11,5298	10,9199	10,3410
12	32,9092	30,3182	28,2997	26,2170	23,3367	21,0261	18,5493	16,9893	15,8120	14,8454	14,0111	13,2661	12,5838	11,9463	11,3403
13	34,5274	31,8830	29,8193	27,6882	24,7356	22,3620	19,8119	18,2020	16,9848	15,9839	15,1187	14,3451	13,6356	12,9717	12,3398
14	36,1239	33,4262	31,3194	29,1412	26,1189	23,6848	21,0641	19,4062	18,1508	17,1169	16,2221	15,4209	14,6853	13,9961	13,3393
15	37,6978	34,9494	32,8015	30,5780	27,4884	24,9958	22,3071	20,6030	19,3107	18,2451	17,3217	16,4940	15,7332	15,0197	14,3389
16	39,2518	36,4555	34,2671	31,9999	28,8453	26,2962	23,5418	21,7931	20,4651	19,3689	18,4179	17,5646	16,7795	16,0425	15,3385
17	40,7911	37,9462	35,7184	33,4087	30,1910	27,5871	24,7690	22,9770	21,6146	20,4887	19,5110	18,6330	17,8244	17,0646	16,3382
18	42,3119	39,4220	37,1564	34,8052	31,5264	28,8693	25,9894	24,1555	22,7595	21,6049	20,6014	19,6993	18,8679	18,0860	17,3379
19	43,8194	40,8847	38,5821	36,1908	32,8523	30,1435	27,2036	25,3289	23,9004	22,7178	21,6891	20,7638	19,9102	19,1069	18,3376
20	45,3142	42,3358	39,9969	37,5663	34,1696	31,4104	28,4120	26,4976	25,0375	23,8277	22,7745	21,8265	20,9514	20,1272	19,3374
21	46,7963	43,7749	41,4009	38,9322	35,4789	32,6706	29,6151	27,6620	26,1711	24,9348	23,8578	22,8876	21,9915	21,1470	20,3372
22	48,2676	45,2041	42,7957	40,2894	36,7807	33,9245	30,8133	28,8224	27,3015	26,0393	24,9390	23,9473	23,0307	22,1663	21,3370
23	49,7276	46,6231	44,1814	41,6383	38,0756	35,1725	32,0069	29,9792	28,4288	27,1413	26,0184	25,0055	24,0689	23,1852	22,3369
24	51,1790	48,0336	45,5584	42,9798	39,3641	36,4150	33,1962	31,1325	29,5533	28,2412	27,0960	26,0625	25,1064	24,2037	23,3367
25	52,6187	49,4351	46,9280	44,3140	40,6465	37,6525	34,3816	32,2825	30,6752	29,3388	28,1719	27,1183	26,1430	25,2218	24,3366
26	54,0511	50,8291	48,2898	45,6416	41,9231	38,8851	35,5632	33,4295	31,7946	30,4346	29,2463	28,1730	27,1789	26,2395	25,3365
27	55,4751	52,2152	49,6450	46,9628	43,1945	40,1133	36,7412	34,5736	32,9117	31,5284	30,3193	29,2266	28,2141	27,2569	26,3363
28	56,8918	53,5939	50,9936	48,2782	44,4608	41,3372	37,9159	35,7150	34,0266	32,6205	31,3909	30,2791	29,2486	28,2740	27,3362
29	58,3006	54,9662	52,3355	49,5878	45,7223	42,5569	39,0875	36,8538	35,1394	33,7109	32,4612	31,3308	30,2825	29,2908	28,3361