UNIVERSIDAD AUTÓNOMA DEL ESTADO DE MÉXICO

FACULTAD DE INGENIERÍA

ANÁLISIS DE LA CRIPTOGRAFÍA CUÁNTICA: ESTADO DEL ARTE Y PERSPECTIVAS

TESINA

QUE PARA OBTENER EL TÍTULO DE

INGENIERA EN COMPUTACIÓN

PRESENTA:

ALMA DANIELA ROMERO DÍAZ

ASESOR:

DR. MARCELO ROMERO HUERTAS

TOLUCA, MÉXICO OCTUBRE 2025

RESUMEN

En esta tesina se presenta un análisis del estado del arte y las perspectivas de la criptografía cuántica. Se aborda desde los conceptos y algoritmos de criptografía clásica y moderna, hasta el desarrollo de criptografía cuántica y post cuántica.

La información presentada busca explicar cómo los algoritmos cuánticos como Shor y Grover representan una amenaza para los criptosistemas tradicionales como AES, DES, 3DES y RSA. Por otra parte, se analizan los algoritmos cuánticos que ofrecen una solución prometedora para proteger la información transmitida por canales clásicos como es el caso del protocolo BB84. Con el análisis teórico que se presenta en esta tesina, se encuentra que, a pesar de que las soluciones para la seguridad en la información aún existen limitaciones tecnológicas que dificultan la implementación práctica de estos avances.

Por consiguiente, aunque la teoría ha demostrado ser prometedora, su ejecución en el uso cotidiano de las personas dependerá de los avances tecnológicos que van surgiendo.

En este documento se ofrece una visión integral sobre el funcionamiento de los algoritmos clásicos, modernos y cuánticos; los obstáculos que enfrentan los algoritmos mencionados; y así como las oportunidades que se presentan en este campo.

TABLA DE CONTENIDO

INDICE DE TABLAS

INDICE DE FIGURAS

INTRODUCCIÓN

Las interconexiones entre dispositivos han aumentado, intercambiando grandes cantidades de datos día a día, desde transacciones bancarias hasta comunicaciones personales son un papel muy importante para la protección de datos sensibles. Con los avances tecnológicos, transmitir información puede ser inseguro, por lo que la creación de técnicas de encriptación es una necesidad primordial. Sin embargo, el surgimiento de una nueva era cuántica trae consigo la pregunta si es una amenaza para los criptosistemas tradicionales o fortalece la protección de los datos, generando interés en la investigación en este campo de estudio.

Actualmente en las empresas ocupan diferentes algoritmos de la criptografía moderna y aun así han sido víctimas de ataques cibernéticos, es importante buscar nuevas alternativas para la protección de información siempre y cuando se considere factible hacia los usuarios.

La criptografía ha evolucionado desde los cifrados manuales, también conocidos como cifrados clásicos. Tal es el caso del cifrado César y el cifrado Vigenère, hasta los avanzados algoritmos de la era moderna, como AES, DES, 3DES y RSA. Por otro lado, del desarrollo de la mecánica cuántica surgió la criptografía cuántica, una nueva alternativa de solución teórica para garantizar la confidencialidad, la integridad y la disponibilidad de los datos (triada CIA). En paralelo evolucionó la mecánica cuántica, creando algoritmos cuánticos como el algoritmo Shor y el algoritmo Grover de los cuales ponen en riesgo los métodos actuales y planteando nuevos retos de la protección de la información.

Dichos algoritmos cuánticos que se han puesto en práctica con cantidades mínimas a las expuestas teóricamente han desatado una nueva investigación, la criptografía post cuántica, un esquema hibrido, consta del uso de los criptosistemas tradicionales con protocolos cuánticos especializados en la distribución de llaves cuánticas (QKD) como es el protocolo BB84.

Esta tesina buscar describir los tipos de la criptografía cuántica incluyendo los sistemas criptográficos clásicos, modernos, cuánticos y post-cuanticos, así como destacando los conceptos fundamentales y la descripción de cada uno de los algoritmos.

Objetivo general

Analizar el estado actual y las perspectivas de la criptografía cuántica en el ámbito de la seguridad de los datos, considerando su origen, evolución y tendencias futuras.

Alcance y limitaciones

La seguridad de la información es un tema relevante en el área de las redes y la comunicación de datos. Por su naturaleza, se convierte en un punto crítico para procurar la confidencialidad, integridad y disponibilidad de los datos de cualquier organización.

El alcance de este trabajo fue determinado con base en la literatura publicada y accesible en el estado del arte.

Organización del documento

El contenido de este trabajo de tesina está estructurado de la siguiente forma:

El Capítulo I describe los antecedentes relacionados al tema de estudio. Considerando el origen, el desarrollo y las tendencias futuras de la ciberseguridad.

El Capítulo II documenta los fundamentos y estado actual de la ciberseguridad basados en algoritmos de criptografía cuántica.

El Capítulo III muestra las tendencias futuras de la ciberseguridad basada en ciberseguridad con algoritmos de criptografía cuántica.

Finalmente, se presenta una sección de conclusiones donde se describen los hallazgos principales de este trabajo.

CAPÍTULO I. CRIPTOGRAFÍA Y SEGURIDAD DE LOS DATOS

Este capítulo presenta los fundamentos de la criptografía, desde sus orígenes clásicos hasta los enfoques modernos, así como la explicación de criptosistemas que se utilizan en la actualidad.

1.1. CONCEPTOS BÁSICOS

La protección de la información es un desafío constante en el ámbito de la ciberseguridad. La ciberseguridad según Stallings [47], es la protección de la información que se almacena, transmite y procesa en un sistema en red de computadoras, otros dispositivos digitales y dispositivos de red y líneas de transmisión, incluido Internet. De la cual se definen dos categorías:

- **Seguridad de la información:** Referente a la preservación de la confidencialidad, integridad y disponibilidad de la información.
- **Seguridad de la red:** Se refiere a la garantía de que la red realiza correctamente sus funciones críticas y que no existen efectos secundarios dañinos.

Hoy en día, con la evolución de la comunicación y los descubrimientos del manejo de la información es más común que viajen a través de la red lo cual es fundamental cumplir con la tríada de seguridad de la información, conocida como CID o CIA (por sus siglas en inglés, enunciando 3 conceptos importantes Confidencialidad, Integridad y Disponibilidad.

Popescul [24] define a esos conceptos de la siguiente forma:

- Confidencialidad de la información, ofrecer acceso solo a las personas autorizadas.

- Integridad, conservar en su forma correcta y completa los datos sin modificaciones no autorizadas, ya sea accidentalmente o a propósito.
- Disponibilidad, asegurar el acceso para los usuarios autorizados, en cualquier momento.

Para garantizar la confidencialidad existen algunas alternativas como son el cifrado de los datos, la autenticación o el control de acceso, Popescul [24] enlista otras medidas para preservar la confidencialidad de los datos e información:

- Clasificar de los datos según su importancia, en varios niveles, que varían desde público hasta privado.
- Otorgar autorizaciones y derechos de acceso a los empleados según la naturaleza de su trabajo, sus competencias, el nivel de clasificación de los datos e información con los que trabajan.
- Aplicar las leyes en vigor específicas del campo de actividad de la organización.
- Firmar contratos de confidencialidad.
- Utilizar contraseñas, técnicas de cifrado, cerraduras y llaves, así como cajas fuertes.

De mismo modo, para la integridad existen métodos como el hash o la suma de comprobación, ambos usados para la detección de errores o manipulación de datos; en este sentido Popescul [24] enuncia algunas medidas para mantener la integridad de los datos e información:

- Mecanismos para verificar los datos con el fin de prevenir que ocurran errores.
- Copias de seguridad.
- Control de acceso.
- Capacitación de los empleados.

También debe haber mantenimiento constante del sistema operativo y software al igual que tener copias de seguridad para que los usuarios puedan acceder en cualquier momento.

Por su parte, Popescul [24] propone mantener a punto el equipo hardware y las redes, conservando copias de seguridad, y el cumplimiento de las leyes.

Autores como Stallings [47], enlista los siguientes mecanismos de seguridad:

- ***Algoritmos criptográficos:*** Son los mecanismos criptográficos reversibles e irreversibles.
    - Mecanismos criptográfico reversible, algoritmo que permite el cifrado y descifrado de los datos.
    - Mecanismos criptográficos irreversibles, incluyen algoritmos de hash y códigos de autenticación de mensajes, típicamente utilizado en aplicaciones de firma digital y autenticación de mensajes.
- ***Integridad de los datos:*** Garantiza la integridad de una unidad de datos o de un flujo de unidades de datos.
- ***Firma digital:*** Datos que permite al receptor de la unidad de datos probar la fuente y la integridad de la información y protegerse contra la falsificación.
- ***Intercambio de autenticación:*** Garantizar la identidad de una entidad mediante el intercambio de información.
- ***Relleno de tráfico (traffic padding):*** Añade bits en los espacios de un flujo de datos para obstaculizar los intentos de análisis del tráfico.
- ***Control de enrutamiento:*** Consiste en elegir rutas seguras, ya sea rutas física o lógicas, para el envío de los datos y permite cambios en el enrutamiento en caso de detectar alguna sospecha de una violación de seguridad.
- **Notarización:** Implementar un tercero de confianza para garantizar ciertas características de un intercambio de datos.

- ***Control de acceso:*** Regulan y garantiza el cumplimiento de los derechos de acceso a los recursos.

De acuerdo con los mecanismos de seguridad, la criptografía ha sido una herramienta clave para garantizar la seguridad de los datos a lo largo del tiempo, evolucionando desde métodos rudimentarios hasta complejos algoritmos modernos. En este capítulo, exploran los fundamentos de la criptografía, abordando tanto los métodos clásicos como las técnicas modernas utilizadas en la actualidad para proteger la información frente a diversas amenazas.

El concepto de criptografía surge a partir de cubrir las necesidades de seguridad en la información, como una técnica basada en algoritmos matemáticos para ocultar información a personas no autorizadas para acceder a ellas. Dos definiciones relevantes se distinguen aquí:

Silve y Nuñez [3] mencionan a la criptografía clásica como un campo de las matemáticas y la ciencia de la computación que estudia los principios y técnicas para cifrar información de forma que solo las personas acreditadas puedan acceder a ella.

Por su parte, Ghute y Suryawanshi [11] conceptualizan a la criptografía como una técnica fundamental y eficaz para la transmisión confiable de datos convirtiendo el texto plano en datos cifrados, conocidos como texto cifrado en dos enfoques principales, la clave simétrica y clave asimétrica, los cuales se definirán más adelante.

La criptografía según Stallings [47], puede dividirse en tres categorías:

- ***Sin clave:*** No ocupa clave durante las transformaciones criptográficas, por ejemplo, la función hash.
- ***De clave única:*** El proceso de transformación depende tanto de los datos de entrada como de una clave secreta, por ejemplo, los algoritmos de cifrado simétrico.

- ***De dos claves:*** Se emplean dos claves distintas y relacionadas en las fases del cálculo, conocidas como clave pública y clave privada, por ejemplo, los algoritmos de cifrado asimétrico.

En el enfoque de cifrado convencional, el objetivo de interrumpir la seguridad regularmente no es solo descifrar el mensaje sino también obtener la clave en uso. En este sentido, existen dos ataques característicos en un cifrado convencional [47]:

- Criptoanálisis: Se aprovecha de las propiedades o debilidades del algoritmo para tratar de determinar el texto original o la clave que se está utilizando.
- Ataque de fuerza bruta: Se prueban las n-posibles combinaciones para formar una clave sobre un texto cifrado hasta obtener el mensaje original.

A lo largo de este trabajo se describirán algunas técnicas que en su mayoría han sido catalogadas como ***estándares*** [47] por instituciones como:

- NIST (Instituto Nacional de Estándares y Tecnología): Se ocupa de la ciencia de la medición, estándares y tecnología para el uso gubernamental y sector privado en EE.UU.
- ISOC (Internet Society): Desarrolla estándares de Internet y especificaciones relacionadas.
- UIT-T (Unión Internacional de Telecomunicaciones – Sector de Normalización de Telecomunicaciones): Organización internacional en donde el gobierno y sector privado coordina redes y servicios de telecomunicaciones a nivel global.
- ISO (Organización Internacional de Estándares): Federación mundial que promueve el desarrollo de la normalización.

1.2. CRIPTOGRAFÍA CLÁSICA

Desde el Imperio Romano, figuras políticas como Julio Cesár en los años 90 a. C., utilizaban métodos simples de cifrado como es la sustitución de letras para la protección de sus mensajes. Consecuentemente de este cifrado, el año 1586 surgió el cifrado Vigenère con un desplazamiento variado en cada letra teniendo como finalidad una mayor complejidad para descifrar el mensaje en caso de no contar con la autorización. Mas adelante, durante la segunda guerra mundial (1939-1945) se volvió un término más común y una herramienta fundamental, utilizando la encriptación y desencriptación de los mensajes militares para una mayor ventaja frente a los contrarios.

El algoritmo César según cuenta Suetonio en Vida de los Césares [27] enviaba mensajes a sus generales utilizando el cifrado por sustitución donde la letra en el texto era sustituida 3 posiciones más ***(Figura 1)***.

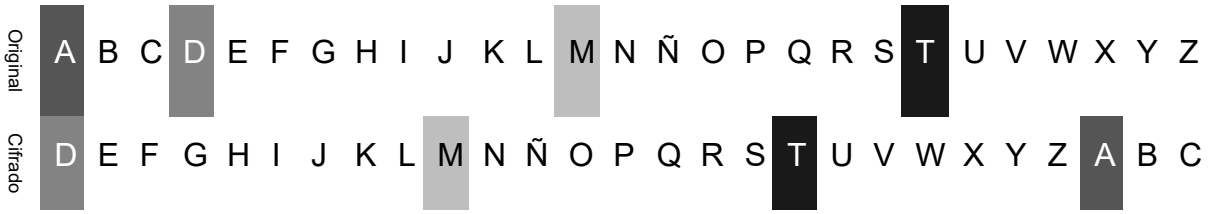

Figura 1. Alfabeto con 3 posiciones más

Ejemplo ***(Figura 2)***:

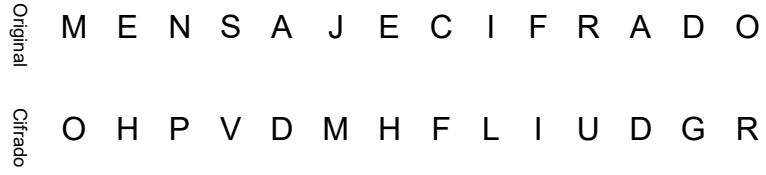

Figura 2. Ejemplo de mensaje cifrado por el cifrado Cesar

Actualmente este cifrado puede variar el número de posiciones, lo cual se le conoce como la *llave* y es necesaria para poder descifrar el *texto cifrado,* es decir, el texto codificado y obtener el *texto llano* que es el texto original o el mensaje que se desea transmitir, ya que el alfabeto contiene 27 letras, el mensaje podía ser descifrado realizando el proceso con las 27 combinaciones correspondientes hasta obtener un mensaje legible, por lo que surge un nuevo método *la cifra Vigenère.*

La cifra Vigenère es un método similar al cifrado César, con la diferencia que la llave es variable con la finalidad que si una letra se repite no tengan la misma letra cifrada ***(Figura 3)***:

Llave: 20-5-7-22-19-16

Original	M	E	N	S	A	J	E	C	I	F	R	A	D	O
Llave	20	5	7	22	19	16	20	5	7	22	19	16	20	5
Cifrado	F	J	T	Ñ	S	Y	X	H	O	A	J	P	W	T

Figura 3. Ejemplo de mensaje cifrado por cifra Vigenère

Como se muestra en el ejemplo de la ***Figura 3*** la llave 20-5-7-22-19-16, si sustituimos el número de la posición por la letra correspondiente en el alfabeto podría ser una palabra, la cual para este ejemplo es *seguro **(Figura 4)**.*

Llave	S	E	G	U	R	O
Posición	20	5	7	22	19	16

Figura 4. Posiciones de acuerdo con la llave

Así mismo, este método de cifrado por sustitución solía ser complicado de descifrar ya que como se muestra en el ejemplo para el caso de la letra *a* son cifradas con distinta letra (S y P) al igual que con la letra *e* (J y X) lo que complicaba interpretar el mensaje. Sin embargo, después de dos siglos en 1854, Charles Babagge (1792-1871) descubrió un método que comprometía la seguridad del cifrado Vigenère, sin embargo, fue hasta 1863 que fue publicada por Kasinski (1805-1881).

1.3. CRIPTOGRAFÍA MODERNA

En esta sección se describen dos técnicas de criptografía moderna, la criptografía simétrica y la criptografía asimétrica.

1.3.1. CRIPTOGRAFIA SIMETRICA

Los primeros criptosistemas ocupaban la criptografía simétrica, de acuerdo con Ghute y Suryawanshi [11] este tipo de criptosistema funciona en el lado del transmisor, los datos de entrada (texto plano), se cifran utilizando una secuencia de código llamada clave. Esos datos cifrados (texto cifrado) se transmite a través del canal de comunicación, que puede ser alámbrico, inalámbrico o incluso una red digital. En el lado del receptor, el texto cifrado se convierte en texto plano al descifrar los datos utilizando la misma clave como se muestra en la ***Figura 5***.

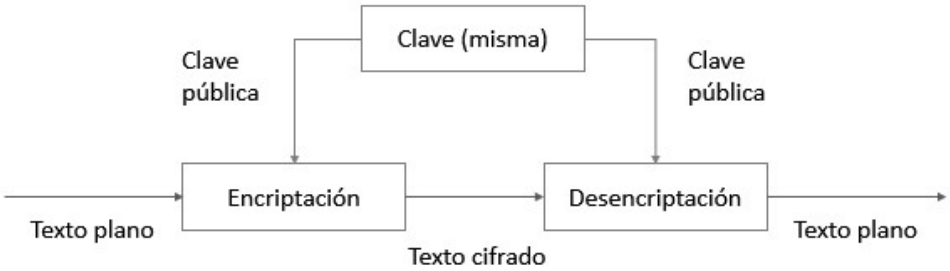

Figura 5. Criptografía Simétrica

De acuerdo con los autores Silva y Nuñez [3], el criptosistema simétrico más conocido es el AES (Estándar de Cifrado Avanzado), un algoritmo de sustitución-permutación que ocupa operaciones matemáticas. Es importante hacer notar que existen otros relevantes como son DES, 3DES, RC4 o Blowfish, aunque, en el presente trabajo solo se abordarán AES, DES y 3DES.

En 1976, las agencias gubernamentales utilizaron el algoritmo DES el cual consiste en un texto plano y una clave de 64 bits. Tomando en cuenta que la clave se reduce a 56 bits, ocupando los 8 bits restantes para fines de verificación de paridad, se realiza una *permutación inicial (ip)* sobre el texto plano de 64 bits, para mezclar los bits. Después de la *ip*, los 64 bits de datos se dividen en dos: 32 bits de texto plano izquierdo y 32 bits de texto plano derecho. Se procesan 16 rondas, cada ronda de cifrado involucra sustitución, permutación y XOR para aumentar la imprevisibilidad. Finalizando las 16 rondas de cifrado, se realiza una permutación final y se genera el texto cifrado [17].

En 1994, NIST confirmó la validez de DES para su uso en el ámbito federal durante cinco años más y sugirió emplearlo únicamente en aplicaciones que no requieran la protección de información clasificada [47].

A continuación se describe un ejemplo del proceso del algoritmo DES basado de autor Larragan [30] en tres pasos:

Paso 1: Como se muestra en la ***Figura 6***, se realiza el cálculo de las 16 subclaves (K_i) de 48 bits cada una, ya que son 16 rondas las que se deben realizar.

(C_O)= bits de la mitad izquierda
(D_O)= bits de la mitad derecha

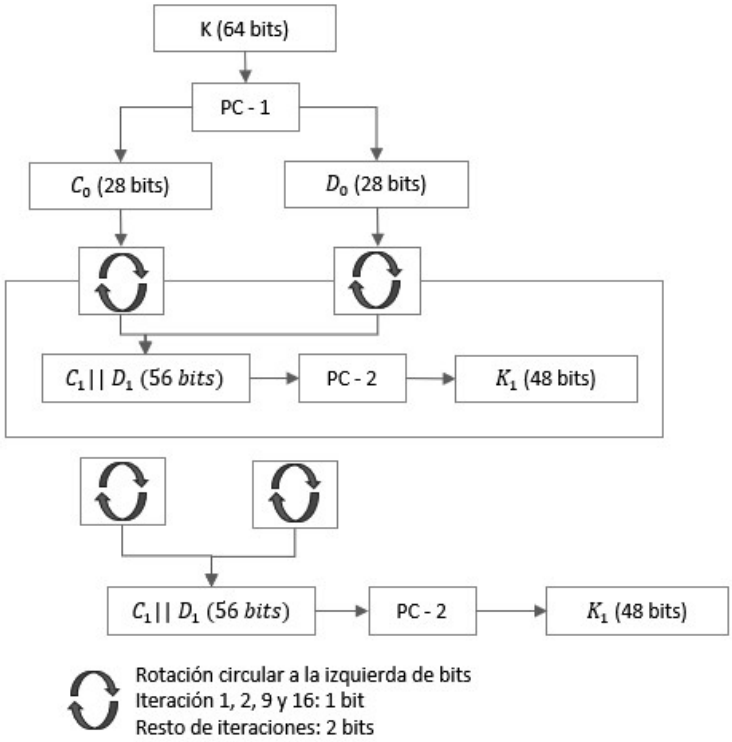

Figura 6. Diagrama de bloques: Creación de las subclaves

1a. Se realiza la permutación de los bits K conforme a la ***Tabla 1*** considerando 56 bits, ya que se eliminan 8 bits menos significativos de cada byte (8, 16, 24, 32, 40, 48, 56 y 64).

PC-1							
57	49	41	33	25	17	9	C_0
1	58	50	42	34	26	18	
10	2	59	51	43	35	27	
19	11	3	60	52	44	36	
63	55	47	39	31	23	15	D_0
7	62	54	46	38	30	22	
14	6	61	53	45	37	29	
21	13	5	28	20	12	4	

Tabla 1. Permutación de subclaves

1b. Se van rotando circularmente a la izquierda conforme al número de bits de la ***Tabla 2***.

Iteración	Número de bits a desplazar
1	1
2	1
3	2
4	2
5	2
6	2
7	2
8	2
9	1
10	2
11	2
12	2
13	2
14	2
15	2
16	1

Tabla 2. Número de bits a desplazar dependiendo de la iteración

1c. Posteriormente al tener los valores binarios de C_i y D_i se realiza la segunda permutación de acuerdo con la ***Tabla 3***.

PC-2					
14	17	11	24	1	5
3	28	15	6	21	10
23	19	12	4	26	8
16	7	27	20	13	2
41	52	31	37	47	55
30	40	51	45	33	48
44	49	39	56	34	53
46	42	50	36	29	32

Tabla 3. Segunda permutación de las subclaves

Paso 2. Para realizar el cifrado del texto, se debe realizar permutación de expansión, operación lógica XOR e uso de S-cajas los cuales se ilustran de manera general en la ***Figura 7,*** sin embargo serán explicados más a detalle a continuación:

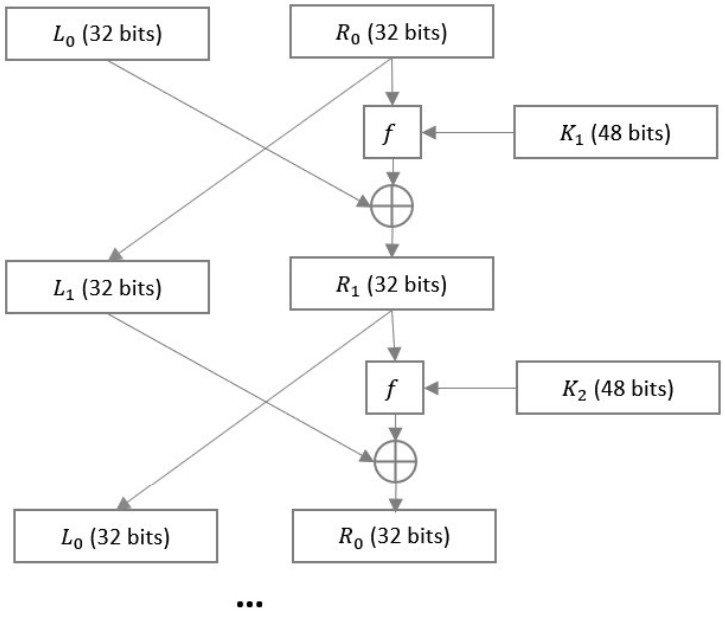

Figura 7. Diagrama de bloques del algoritmo DES

Primero se trabaja con R_i, mismo que se utiliza para la función f ***(Figura 8)*** donde se realizará una permutación de expansión (E), la cual realizará la transformación del bloque de 32 bits de entrada en uno de 48 bits para la salida, como se explica en el paso 2a.

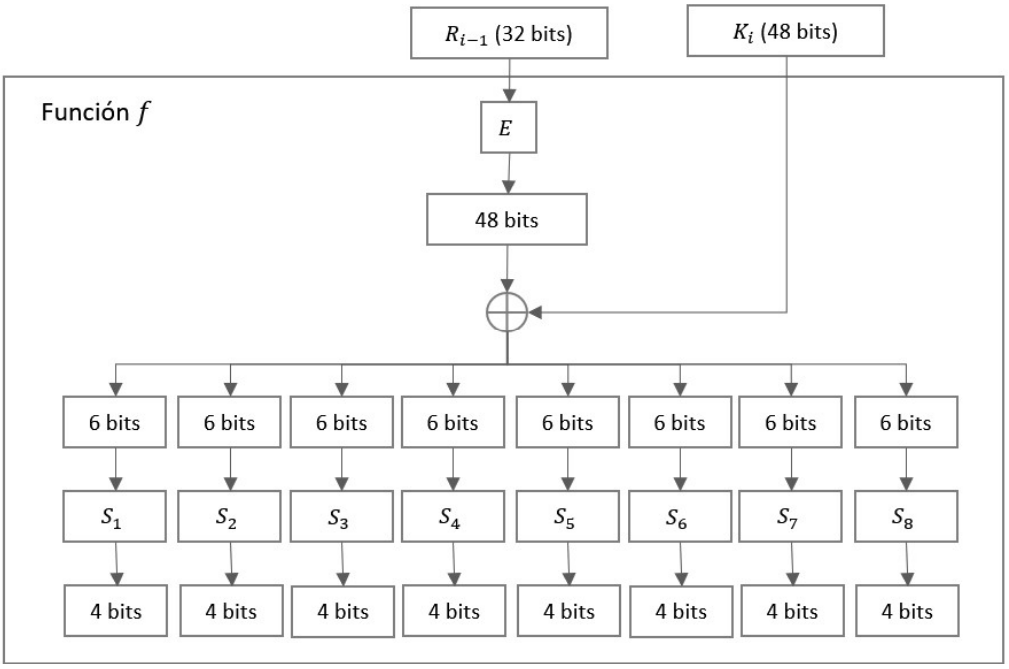

Figura 8. Diagrama de bloques de la función f

2a. La permutación de expansión (E) se conforma de los bits de entrada en la posición de que se muestra en la ***Tabla 4***, duplicando bits para poder obtener los 48 bits de salida.

E					
32	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	1

Tabla 4. Permutación de expansión E

2b. Se realiza la operación XOR con el valor de la subclave, posteriormente a tener el resultado de 48 bits se realiza una separación por cada 6 bits para los cuales nuevamente hay que reducir a 32 bits para repetir el proceso hasta completar las 16 rondas ***(Figura 9)***.

(R_i)= es el lado derecho del texto (32 bits)

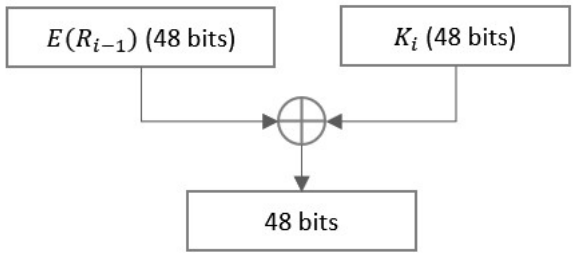

Figura 9. Diagrama de flujo para obtener el siguiente R_i

2c. Cuando se obtienen los 8 bloques de 6 bits, se realiza las tablas de S-Cajas como se muestra en las ***Tablas 5 a la 12***, con estas tablas se obtiene un número por cada una, el cual se encuentra teniendo en cuenta lo siguiente:

- Fila: Primer y último digito del bloque de 6 bits
- Columna: Del segundo al quinto valor
- Número (Por encontrar): Valor del número en la posición de la fila y la columna.

S_1	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
1	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
2	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
3	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

Tabla 5. S_1- Cajas del algoritmo DES

S_2	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
1	3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
2	0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
3	13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9

Tabla 6. S_2- Cajas del algoritmo DES

S_3	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8
1	13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1
2	13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7
3	1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12

Tabla 7. S_3- Cajas del algoritmo DES

S_4	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15
1	13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9
2	10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
3	3	15	0	6	1 0	1	13	8	9	4	5	11	12	7	2	14

Tabla 8. S_4- Cajas del algoritmo DES

S_5	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9
1	14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6
2	4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14
3	11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3

Tabla 9. S_5- Cajas del algoritmo DES

S_6	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11
1	10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8
2	9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6
3	4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13

Tabla 10. S_6- Cajas del algoritmo DES

S_7	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1
1	13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6
2	1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2
3	6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12

Tabla 11. S_7- Cajas del algoritmo DES

S_8	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7
1	1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2
2	7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8
3	2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11

Tabla 12. S_8- Cajas del algoritmo DES

2d. Con los 8 números obtenidos en las cajas del paso 2c, se convierten a sistema binario y se acomodan los valores conforme a la ***Tabla 13***, una vez obtenida la tabla correspondiente, se aplica una operación lógica XOR con L_i ***(Figura 7)*** y repetir con el resultado desde el paso 2.b. hasta realizar las 16 rondas.

P			
16	7	20	21
29	12	28	17
1	15	23	26
5	18	31	10
2	8	24	14
32	27	3	9
19	13	30	6
22	11	4	25

Tabla 13. Permutación final de cada ronda

Paso 3. Finalmente, se realiza la permutación inversa mostrada en la ***Tabla 14*** con lo obtenido en la última ronda R_{16} y L_{16} y este sería el resultado final del mensaje cifrado.

IP^{-1}							
40	8	48	16	56	24	64	32
39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30
37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28
35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26
33	1	41	9	49	17	57	25

Tabla 14. Permutación inversa

Ahumada-Urquijo et al. [31] mencionan que con el paso del tiempo se encontraron debilidades de seguridad y eficiencia al algoritmo por lo que surge, en el año 1999 NIST publicó una nueva versión del estándar DES conocido como algoritmo 3DES el cual aumenta la seguridad, sin embargo, se considera un algoritmo lento ya que el proceso es realizado tres veces de forma secuencial:

- Cifrado con la primera clave.
- Descifrado con la segunda clave.
- Cifrado nuevamente con la tercera clave.

Actualmente, este algoritmo puede ocupar dos o tres claves diferentes, sin embargo, el NIST recomienda solamente el uso del algoritmo 3DES de tres claves, reforzando la seguridad con una llave de 168 bits ($3 \times 56\ bits$) en lugar de la llave 112 bits ($2\times 56\ bits$) que proporciona el algoritmo 3DES de dos claves [47].

Posteriormente en 2001, se aplicó el algoritmo AES, un algoritmo similar al DES, pero ocupando una clave completa de 64 bits y un texto de 128 bits, el cual se divide en una matriz de 4x4 conocida como la matriz de estado, donde cada elemento de la matriz es un byte [17].

En la ***Figura 10*** se muestra el algoritmo que opera con 10, 12 o 14 rondas de acuerdo con el tamaño de la clave 128, 192 y 256 respectivamente, de acuerdo con Martínez [32], cada ronda se forma en 4 capas:

- Byte substitution layer
- ShiftRows layer
- MixColumn layer
- Key addition layer

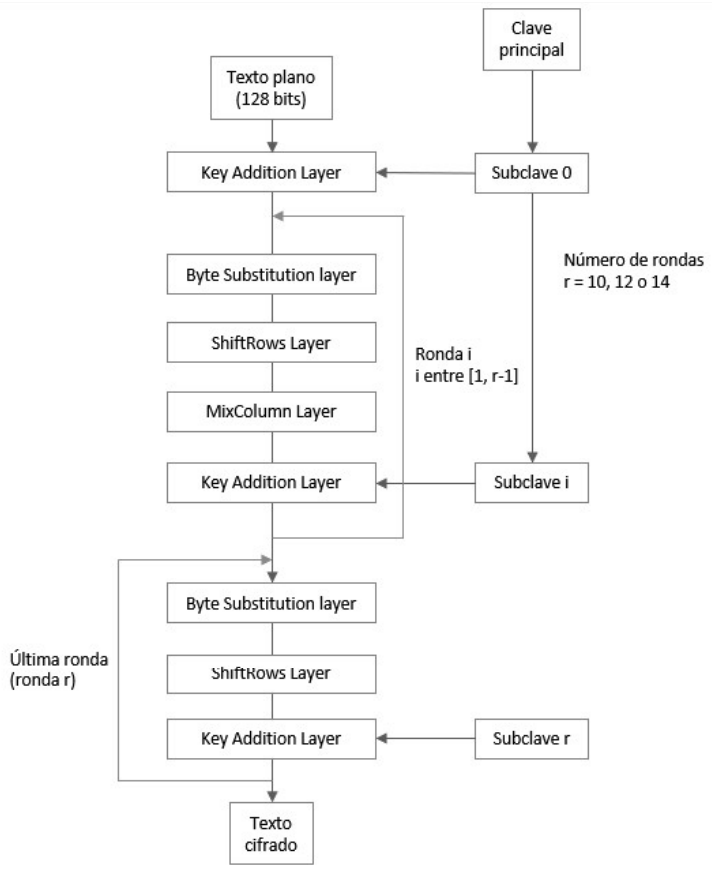

Figura 10. Diagrama de bloques del algoritmo AES

La primera etapa de cada ronda es *Byte substitution layer,* en la cual se sustituye cada byte por el valor asignado en las S-*cajas* ***(Tabla 15),*** donde primeramente hay que convertir el valor binario a Hexadecimal sobre los 16 bytes de la matriz de estado.

	0	*1*	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*A*	*B*	*C*	*D*	*E*	*F*
0	*63*	*7C*	*77*	*7B*	*F2*	*6B*	*6F*	*C5*	*30*	*01*	*67*	*2B*	*FE*	*D7*	*AB*	*76*
1	*CA*	*82*	*C9*	*7D*	*FA*	*59*	*47*	*F0*	*AD*	*D4*	*A2*	*AF*	*9C*	*A4*	*72*	*C0*
2	*B7*	*FD*	*93*	*26*	*36*	*3F*	*F7*	*CC*	*34*	*A5*	*E5*	*F1*	*71*	*D8*	*31*	*15*
3	*04*	*C7*	*23*	*C3*	*18*	*96*	*05*	*9A*	*07*	*12*	*80*	*E2*	*EB*	*27*	*B2*	*75*
4	*09*	*83*	*2C*	*1A*	*1B*	*6E*	*5A*	*A0*	*52*	*3B*	*D6*	*3B*	*29*	*E3*	*2F*	*84*
5	*53*	*D1*	*00*	*ED*	*20*	*FC*	*B1*	*5B*	*6A*	*CB*	*BE*	*39*	*4A*	*4C*	*58*	*CF*
6	*D0*	*EF*	*AA*	*FB*	*43*	*4D*	*33*	*85*	*45*	*F9*	*02*	*F7*	*50*	*3C*	*9F*	*A8*
7	*51*	*A3*	*40*	*8F*	*92*	*9D*	*38*	*F5*	*BC*	*B6*	*DA*	*21*	*10*	*FF*	*F3*	*2D*
8	*CD*	*0C*	*13*	*EC*	*5F*	*97*	*44*	*17*	*C4*	*A7*	*7E*	*3D*	*64*	*5D*	*19*	*73*
9	*60*	*81*	*4F*	*DC*	*22*	*2A*	*90*	*88*	*46*	*EE*	*B8*	*14*	*DE*	*5E*	*0B*	*DB*
A	*E0*	*32*	*3A*	*0A*	*49*	*06*	*24*	*5C*	*C2*	*D3*	*AC*	*62*	*91*	*95*	*E4*	*79*
B	*E7*	*C8*	*37*	*6D*	*8D*	*D5*	*4E*	*A9*	*6C*	*56*	*F4*	*EA*	*65*	*7A*	*AE*	*08*
C	*BA*	*78*	*25*	*2E*	*1C*	*A6*	*B4*	*C6*	*E8*	*DD*	*74*	*1F*	*4B*	*BD*	*8B*	*8ª*
D	*70*	*3E*	*B5*	*66*	*48*	*03*	*F6*	*0E*	*61*	*35*	*57*	*B9*	*86*	*C1*	*1E*	*9E*
E	*E1*	*F8*	*98*	*11*	*69*	*D9*	*E8*	*94*	*9B*	*1E*	*87*	*E9*	*CE*	*55*	*28*	*DF*
F	*8C*	*A1*	*89*	*0D*	*BF*	*E6*	*42*	*68*	*41*	*99*	*2D*	*0F*	*B0*	*54*	*BB*	*16*

Tabla 15. S-Cajas algoritmo AES

Para *ShiftRows* se realiza una transformación cíclica sobre la matriz de estado como se muestra en la ***Figura 11***.

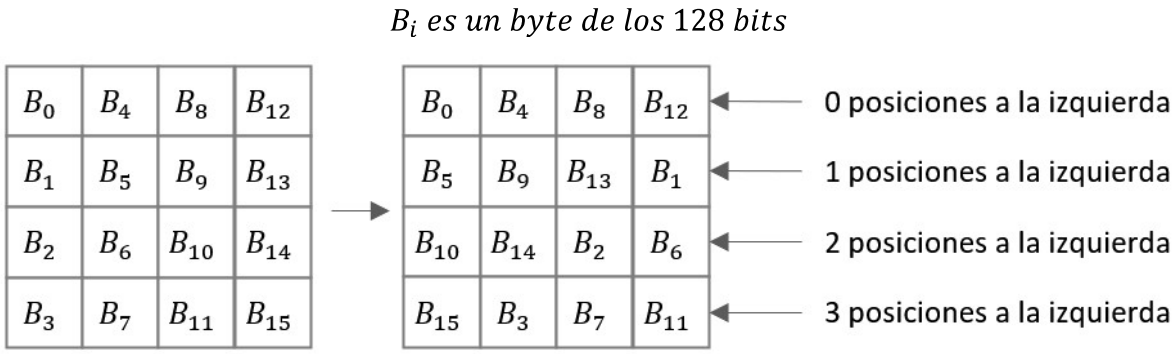

Figura 11. ShiftRows

Posteriormente en la etapa de *MixColumn* ***(Figura 12)***, cada columna de la matriz de estado es multiplicada por una matriz constante establecida por FIPS 197 [46], siendo *01*, *02* y *03* valores hexadecimales.

$$\begin{pmatrix} C_0 \\ C_1 \\ C_2 \\ C_3 \end{pmatrix} = \begin{pmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{pmatrix} \begin{pmatrix} B_0 \\ B_5 \\ B_{10} \\ B_{15} \end{pmatrix}$$

$$\begin{pmatrix} C_4 \\ C_5 \\ C_6 \\ C_7 \end{pmatrix} = \begin{pmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{pmatrix} \begin{pmatrix} B_4 \\ B_9 \\ B_{14} \\ B_3 \end{pmatrix}$$

$$\begin{pmatrix} C_8 \\ C_9 \\ C_{10} \\ C_{11} \end{pmatrix} = \begin{pmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{pmatrix} \begin{pmatrix} B_8 \\ B_{13} \\ B_2 \\ B_7 \end{pmatrix}$$

$$\begin{pmatrix} C_{12} \\ C_{13} \\ C_{14} \\ C_{15} \end{pmatrix} = \begin{pmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{pmatrix} \begin{pmatrix} B_{12} \\ B_1 \\ B_6 \\ B_{11} \end{pmatrix}$$

Figura 12. Multiplicación de Matriz de Estado por Matriz Constante

Finalmente, para la etapa *Key Addition,* con la subclave de esa ronda y la matriz C obtenida en el paso anterior se realiza XOR con la matriz de estado para obtener el resultado de esa ronda, y poder volver a iterar estos procesos hasta llegar al número de iteraciones adecuadas dependiente el tamaño de la clave.

1.3.2. CRIPTOGRAFÍA ASIMETRICA

Suryawanshi [10] describe la criptografía asimétrica como una técnica donde se utilizan dos claves, una para cifrar el texto, y otra para descifrarlo, ver ***Figura 13.***

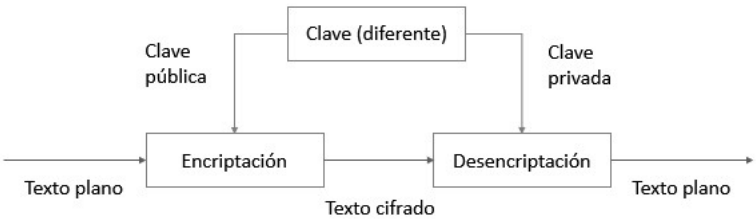

Figura 13. Criptografía asimétrica

El cifrado asimétrico de acuerdo con Stallings [47], tienen una variedad de aplicaciones, destacando:

- *Algoritmo de firma digital,* el cual refuerza la autenticidad de la información.
- *Intercambio de claves*, donde se distribuye de manera segura una clave simétrica a dos o más partes.
- *Autenticación de usuarios*, verifica que un usuario que intenta ingresar a un sistema es legítimo, similarmente, verifica que el sistema también sea legítimo.
- *Cifrado/descifrado,* el ente remitente cifra el mensaje con una clave pública del receptor, y el receptor descifra con la clave privada.

Tanto el cifrado asimétrico como el cifrado simétrico, son vulnerables a ataques de fuerza bruta. Por lo cual, una de las medidas de protección es el uso de claves de hasta 4096 bits, reforzando la seguridad que proporciona la clave publica que depende de una multiplicación de número primos y es irreversible por la complejidad de factorización [47].

En 1977, se creó el criptosistema asimétrico: RSA (son las letras iniciales de Rivest, Shamir, Adleman, los nombres de sus creadores) se basa en la complejidad de factorizar números primos grandes [3], y descubrir la clave privada a partir de la pública. Actualmente, se utiliza el algoritmo de Euclides para factorizar número grandes, pero se necesita un tiempo de cómputo que aumenta exponencialmente con el número de dígitos de n [2].

El algoritmo RSA conforme a Huawei y Aldeco et al. [33][48] consiste primeramente en generar la clave pública y la clave primaria:

1. Seleccionar dos números primos: p, q (pueden ser distintos)
2. Calcular: $n = p \cdot q$
3. Calcular $z = (p-1) \cdot (q-1)$
4. Seleccionar un entero k que cumpla con el Máximo Común Divisor (MCD): $MCD(z,k) = 1; 1 < k < z$
5. Elegir j cumpliendo con $k * j = 1(mod\ z)$ o $j = (1 + x \cdot z) / k$

   Clave Publica: (n, k) Clave Privada: (j)

   Posteriormente se realiza el cifrado, siendo C el texto cifrado
6. $M\wedge k = C\ (mod\ n); C\ M\wedge k\ \%\ n,$

$$C(M) = M^k\ mod\ n$$

Por otra parte, el descifrado se basa en la expresión

$$D\big(C(M)\big) = M^j\ mod\ n$$

A continuación, se muestra un ejemplo práctico con números pequeños para ilustrar cómo funciona el algoritmo RSA en la generación de claves, tanto en la operación de cifrado y descifrado. Este ejemplo no es seguro en la práctica (ya que usa números primos pequeños), pero permite comprender claramente el procedimiento. En implementaciones reales se emplean claves con longitudes superiores a 2048 bits para garantizar un nivel adecuado de seguridad.

a. Generación de claves RSA

Paso 1: Seleccionar dos números primos distintos

$$p = 5, q = 11$$

Paso 2: Calcular $n = p \cdot q$

$$n = 5 \cdot 11 = 55$$

Paso 3: Calcular $z = (p-1) \cdot (q-1)$

$$z = (5-1) \cdot (11-1) = 40$$

Paso 4: Seleccionar un entero k que cumpla: $MCD(z,k) = 1; 1 < k < z$

$$k = 3 \rightarrow MCD\ (40,3) = 1$$

Paso 5: Elegir j cumpliendo $k * j \equiv 1(mod\ z)$

$$j = 27 \rightarrow 3 \cdot 27 = 81;\ 81\ mod\ 40 = 1$$

Clave publica $(55,3)$

Clave privada j=27

b. Cifrado

Suponiendo que el mensaje a cifrar es M = 7

$$C \equiv M^k mod\ n$$

$$C \equiv 7^3 mod\ 55$$

$$7^3 = 343$$

$$343\ mod\ 55 = 13$$

Texto cifrado: C= 13

c. Descifrado

$$D \equiv M^j mod\ n$$

$$C \equiv 13^{27} mod\ 55$$

$$M = 7$$

Si bien existen otros algoritmos asimétricos como Diffie–Hellman para el intercambio de llaves, ElGamal o los basados en curvas elípticas (ECC) usado para firmas digitales, RSA ha sido uno de los más influyentes y ampliamente implementados en la práctica.

Su fortaleza radica en la dificultad de factorizar números enteros grandes, lo que garantiza un alto nivel de seguridad siempre que se empleen claves de tamaño suficiente.

En marzo de 1991, *RSA Laboratories* lanzó un reto mundial para factorizar 54 números *semi-primos*, promoviendo la investigación en teoría de números y mostrando la dificultad de factorizar números grandes. El reto terminó en 2007 con la factorización de 12 números; y a la fecha, se han factorizado 11 números más, siendo el mayor RSA-250, con 829 bits (250 dígitos). En 2009, se estimó que RSA-1024 podría factorizarse en 10 años, lo que no ocurrió. Por ello, el NIST recomendó desde 2013 usar módulos de 2048 bits en lugar de 1024 [48], e incluso, se recomienda actualmente considerar longitudes superiores como 3072 o 4096 bits para garantizar un mayor nivel de seguridad.

De este modo, la criptografía asimétrica se consolida como un pilar fundamental en la seguridad de la información moderna, con aplicaciones en cifrado, autenticación y firma digital.

1.4. RESUMEN

En este capítulo, se ha proporcionado una breve descripción de información: desde realizar el cifrado sin tecnología mostrando un texto diferente al original, hasta algoritmos avanzados los cuales realizan el cifrado con una mayor dificultad de descifrado sin tener la clave de acceso, garantizando la integridad, confidencialidad y disponibilidad de los datos.

Así mismo, se explicaron los procesos que siguen estos algoritmos para el cifrado de los datos, para comprender su evolución se entiende que los algoritmos simétricos (ocupan una clave compartida) y mientras que los asimétricos ocupan una clave de cifrado diferente a la clave de descifrado.

La información proporcionada en este capítulo ha permitido comprender la evolución de la criptografía y su papel en la seguridad de los datos. Se analizaron los métodos de la criptografía clásica y su transición hacia enfoques más avanzados en la criptografía moderna. Sin embargo, la aparición de la computación cuántica representa un reto significativo para los sistemas criptográficos actuales. En el siguiente capítulo, se introduce el concepto de ciberseguridad cuántica, explorando sus fundamentos, aplicaciones y los algoritmos que amenazan los sistemas tradicionales.

CAPÍTULO II. CIBERSEGURIDAD CUÁNTICA

En este capítulo, se explorarán los orígenes y fundamentos de la ciberseguridad cuántica, la criptografía cuántica y los principales algoritmos cuánticos que desafían la seguridad actual, así como los obstáculos para su implementación.

2.1. ORIGEN

Los equipos de cómputo cuentan con capacidades que le permiten la realización de múltiples operaciones en pocos segundos, lo que permite con mayor facilidad infringir la seguridad de la información. Por esta razón, se crean las técnicas de criptografía cuántica, una combinación de la mecánica cuántica con la criptografía, como medio defensa contra de diversos tipos de amenazas [5] [20].

La criptografía cuántica busca garantizar la seguridad de la información. Se utiliza la física en lugar de las matemáticas, y se basa en las propiedades y principios de la mecánica cuántica, por lo que se obtiene una ventaja en comparación de la criptografía clásica y la criptografía moderna, haciendo casi imposible acceder a los datos a cualquier persona no autorizada [25].

Una de las investigaciones pioneras en la criptografía cuántica es Stephen Wiesner y Gilles Brassard, en 1983, Codificación cuántica conjugada en donde se plantea con su publicación: el almacenamiento y la transmisión observable de dos mensajes codificándolos. Donde, con la polarización lineal y circular de los fotones, se puede cifrar y descifrar cualquiera de los dos, pero no ambos, debido al entrelazamiento cuántico. Esto asegura conexiones seguras entre servidores mientras evita la detección por parte de espías con capacidades computacionales ilimitadas [5] [28].

Años después, en 1991, Bennett sugirió un protocolo de criptografía cuántica basado en las desigualdades de Bell utilizado para los estados entrelazados de dos partículas de Einstein-Podolsky-Rosen (EPR) y demostró que la Distribución Cuántica de Claves (QKD) podría ser factible al generar un prototipo real del protocolo BB84 que utiliza la polarización de fotones [6].

Los protocolos QKD están diseñados para transferir una clave entre partes autorizadas con un nivel de seguridad prácticamente imposible de comprometer, mientras el protocolo BB84 es una forma revolucionaria de codificar información utilizando estados cuánticos ortogonales [22].

2.1.1. FUNDAMENTOS

Para entender la diferencia entre la criptografía moderna y la criptografía cuántica, Kumari et al. [12], dicen que las computadoras clásicas utilizan dígitos binarios para almacenar y procesar información, mientras que las computadoras cuánticas usan bits cuánticos o *qubits* (abreviación en inglés, quantum bit). Estos *qubits* pueden existir en múltiples estados simultáneamente, lo que permite realizar cálculos de manera exponencialmente más rápida.

En la criptografía cuántica, la información se transfiere en *qubits*, unidad mínima de información cuántica, definido como un sistema cuántico que consta de 2 estados observables ***(Figura 14),*** así mismo estos qubits están en superposición de ambos estados al mismo tiempo, lo que dificulta su copia [5] [11].

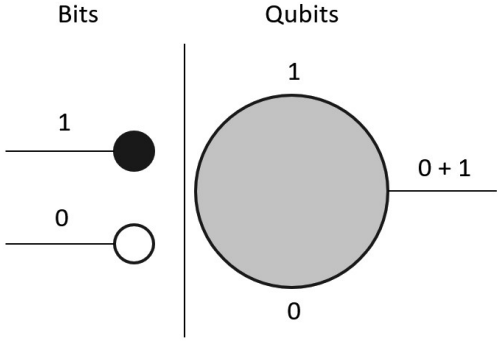

Figura 14. Representación de Qubits

La criptografía cuántica de acuerdo con Sehgal et al. [25][20], está conformada por dos propiedades cuánticas principales:

- Superposición.
- Entrelazamiento.

Sehgal et al. [25] explicaban el concepto de superposición con un ejemplo; supongamos que tenemos dos opciones 5 y 6, si seleccionamos el número 5.1 la probabilidad de elegir 5 es mayor que del número 6. El cálculo de los qubits es la elección de números, ya que para afirmar la dirección antes de medirlos implica que la probabilidad es la misma, puede ser 0 o 1 al mismo tiempo.

El entrelazamiento es otra propiedad que considera las direcciones de giro de dos o más qubits. Dado que ambos qubits están entrelazados entre sí, relacionándose sin importar lo lejos que estén en el universo, los estados de entrelazamiento son cuando los qubits giran en la misma dirección y cuando los qubits giran en dirección opuesta ***(Figura 15)*** [25].

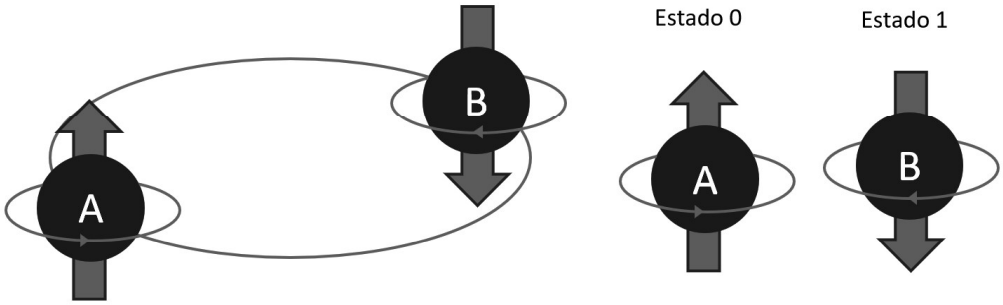

Figura 15. Entrelazamiento

Bishwas y Advani [1] añaden dos propiedades a las mencionadas, las cuales describen de la siguiente manera:

- **Teorema de no clonación:** Este teorema establece que los estados cuánticos no pueden ser copiados. Una vez que se interactúa con el sistema, la superposición colapsará en un solo estado.

- **De-coherencia:** Aunque los estados cuánticos pueden estar en superposición, una vez que medimos el estado al interactuar con él, todo el sistema cuántico colapsará a un solo estado con un valor clásico. No se puede medir múltiples estados cuánticos simultáneamente.

Antes de explicar la QKD, es importante comprender el protocolo de la física cuántica, *principio de incertidumbre de Heisenberg* donde asegura que es imposible determinar con precisión absoluta y de forma simultánea, el valor de dos magnitudes conjugadas de un sistema elemental [36].

2.2. CRIPTOGRAFÍA CUÁNTICA

Teniendo los conceptos fundamentales para entender la Distribución de Claves Cuánticas (QKD, por sus siglas en inglés), Ati [13] destaca el trabajo de Bennett y Brassard, en 1984, los cuales crearon este primer método (QKD) utilizado para distribuir claves de sesión a los usuarios finales el cual fue llamado protocolo BB84.

La QKD es una técnica avanzada que utiliza las propiedades únicas de la física cuántica, como el teorema de no clonación, el principio de incertidumbre de Heisenberg y el entrelazamiento, para proporcionar un nivel de seguridad incomparable [22].

Pedone et al. [34] explica que la QKD depende de un canal cuántico que permite a varios pares intercambiar qubits, generalmente codificados como fotones. Adicionalmente, los protocolos QKD dependen de un canal clásico autenticado público para intercambiar información fuera de banda necesaria para coordinar los pares durante el intercambio.

Así mismo, Pedone et al. [34] mencionan que los sistemas de QKD tienen dos variables:

- *QKD de variable discreta*, también conocido como QKD basado en qubits, realiza la codificación y decodificación utilizando qubits u otros sistemas cuánticos.
- *QKD de variable continua*, las claves se codifican en las cuadraturas del campo electromagnético cuantizado y se descodifica con detecciones coherentes.

En diversas investigaciones se han propuesto muchos protocolos de variable discreta, entre ellas:

- BB84
- SARG04
- COW
- E91
- BBM92

El protocolo más famoso es BB84; Win et al. [26] mencionan que este se base en la polarización de fotones, la misma que utiliza la *base rectilínea* (+) tiene dos polaridades, la horizontal que representa el bit 0 y la vertical el bit 1 y la *base diagonal* (x) igualmente tiene dos polaridades, +45° representa el bit 0 y -45° representa el bit 1 ***(Figura 16)***.

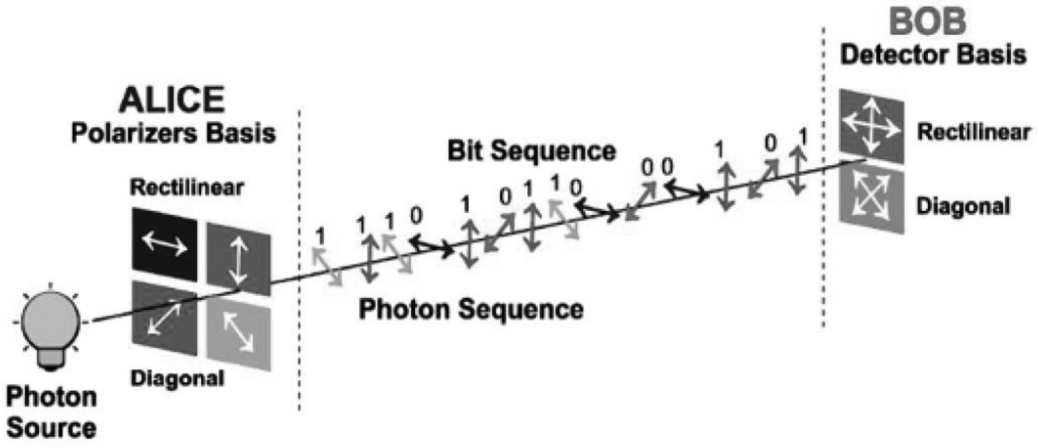

Figura 16. Representación de la QKD [26]

Conforme al autor Ati [13] se explica que el funcionamiento del protocolo consta de codificar cada bit de la clave en el estado de polarización de un solo fotón, así mismo, la distribución cuántica no puede proporcionar un servicio de distribución de claves como infraestructura central a causa de los límites de la computación cuántica, por ejemplo, la distancia de transmisión de qubits y la precisión del detector de qubits.

Rahman y Hossam-E-Haider [35] definen el protocolo BB84 como un ejemplo donde dos actores principales: Alice y Bob, y un tercer actor Eve, el atacante de la seguridad para el robo de información. En el mismo contexto Alice es quien envía el mensaje y Bob el receptor, quien codifica y decodifica la información.

El mensaje del ejemplo anterior se envía en qubits y se miden según diferentes bases, esto depende de quién realiza la medición. Según el principio de incertidumbre Heisenberg, el valor de la base general ($|0\rangle$ y $|1\rangle$) de un qubit simple será diferente del valor de la base de signo ($|+\rangle$ y $|-\rangle$) o de cualquier otra base diferente.

A continuación se muestran los pasos básicos del protocolo BB84 para la distribución cuántica de claves, utilizando a Alice como transmisora, Bob como receptor y Eve como atacante a través de un canal cuántico ***(Figura 17)***:

1. *Emisor*, crea una secuencia de bits y una base (rectilínea o diagonal) aleatorias para codificar cada bit en un qubit. Posteriormente, envía los qubits a *Receptor* a través de un canal cuántico.

2. *Receptor*, recibe los qubits y mide cada qubit eligiendo bases al azar por ejemplo, base diagonal o base rectilínea. Aún sin saber cuál base utilizó *Emisor*.

3. Una vez completada la medición, *Receptor* se comunica con *Emisor* a través de un canal clásico para confirmar que se ha recibido todos los qubits.

4. *Emisor* le indica a *Receptor* la base correcta para medir los qubits. Por lo que *Receptor*, compara sus propias bases con las de *Emisor* y conserva solo los resultados donde ambas bases coincidieron. Esa parte compartida de la secuencia se convierte en la clave secreta. Esta comunicación se realiza a través de un canal de comunicación clásico.

    a. Si un tercero (como *Atacante*) intentó interceptar los qubits, su intervención introducirá errores detectables. *Emisor* y *Receptor* pueden verificar una parte de la clave para comprobar si hubo intrusión.

5. Finalmente, si existe intervención se transmite otra clave a través del canal cuántico, y realizando los mismos pasos anteriores, en caso exitoso la clave se recupera y se decodifica la información.

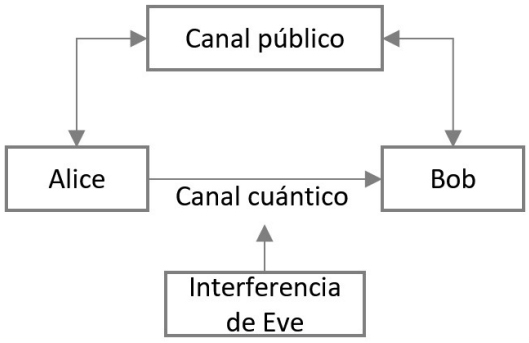

Figura 17. Protocolo BB84

A continuación, se muestra un ejemplo práctico con una secuencia reducida de bits para ilustrar cómo funciona el protocolo BB84 en la distribución de una clave cuántica.

Paso 1:

- Alice establece una secuencia de bits aleatorios, 1010.
- Codifica esos bits y elige bases al azar (rectilínea o diagonal)

- 1° Bit (1): Base rectilínea ↑
- 2° Bit (0): Base diagonal ↗
- 3° Bit (1): Base rectilínea →
- 4° Bit (0): Base diagonal ↘

$$\therefore \text{Bits: } 1,0,1,0 \text{ Bases } \uparrow, \nearrow, \rightarrow, \searrow$$

Paso 2:

- Bob recibe los qubits de Alice, al no saber las bases para medir cada qubits, él propone al azar las siguientes:
  - 1° Bit (1): Base diagonal ↗
  - 2° Bit (0): Base diagonal ↘
  - 3° Bit (1): Base rectilínea →
  - 4° Bit (0): Base rectilínea ↑

$$\therefore \text{Bits: } 1,0,1,0 \text{ Bases } \nearrow, \searrow, \rightarrow, \uparrow$$

- El resultado de Bob sería:
  - 1° Bit (1): Base errónea, resultado es aleatorio (0)
  - 2° Bit (0): Base errónea, resultado aleatorio (1)
  - 3° Bit (1): Base correcta, resultado correcto (1)
  - 4° Bit (0): Base errónea, resultado aleatorio (0)

$$\therefore \text{Bits } : 0,1,1,0$$

Paso 3:

- Bob llama a Alice (canal clásico) y mencionan las bases que usó para medir:
  - Bob: ↗, ↘, →, ↑
  - Alice: ↑, ↗, →, ↘
- Ambos conocen los bits tiene las bases correctas
  - 1°, 2° y 4°; ya que la base fue incorrecta se descartan, no importando que hayan coincidido el resultado de los bits.
  - 3°; se conserva: 1

Paso 4:

- La manera de asegurarse si el canal cuántico es seguro, Alice y Bob comparten públicamente una pequeña parte de los bits compartidos, es decir, en este ejemplo revisan si el tercer bit es 1 para ambos.
- Para esta prueba es necesario que anteriormente hayan coincidido en la base (paso 3), y posteriormente coincidir en el valor del bit, se concluye que no presento espionaje; en caso de existir diferencias Alice y Bob sabrán que alguien (Eve) trató de espiar e interrumpirán el protocolo.

Paso 5:

- Los bits que quedan después de descartar las mediciones incorrectas se utilizaran para la clave final, siendo este caso del 1.
- Ahora con la clave secreta 1, pueden usar para cifrar la información con algún criptosistema moderno.

Adicional al ejemplo anterior, Ricci et al. mencionan que esta distribución puede proporcionar seguridad a largo plazo y no impone límites al poder computacional del adversario, por lo que se puede ocupar como un método complementario, además la QKD posee la capacidad de resistir los ataques de la computación cuántica [19] [23].

Seguido del ejemplo técnico, se presenta una analogía basada en Teleco Renta [49], para comprender el funcionamiento del protocolo BB84 de una manera más sencilla.

Imaginando que se tiene una caja con dos puertas, una puerta en la parte superior (puerta ***a***) y una puerta lateral (puerta ***b***), *como se muestra en la* ***Figura 18****,* así como, una ficha que tienen marcado en un lado el número **1** y del otro lado el número **0.**

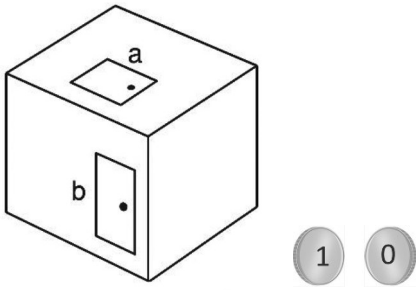

Figura 18. Caja ejemplo del protocolo BB84

Para esta caja, se tienen las siguientes reglas:

- Si la ficha se coloca por la *puerta a* con el lado 1 hacia arriba, cada vez que se observe por esa puerta, se verá el 1.
- Si alguien observa la *puerta b*, hay un 50% de probabilidad de ver 0 o 1; el resultado es aleatorio.
- Lo mismo ocurre si la ficha se inserta por la *puerta b*: solo la puerta correspondiente garantiza una lectura correcta; por la otra, el resultado es aleatorio.

Supóngase que Alice envía 10 bits a Bob, eligiendo aleatoriamente porque "puerta" se insertan los bits, es decir, se decide la base a utilizar ***(Figura 19)***.

	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
Bit	1	1	0	1	0	0	0	1	1	0
Puerta	↑	→	→	↑	↑	→	↑	↑	→	→

Figura 19. Selección de bases y envío de qubits

Bob sin conocer qué base usó Alice, mide los qubits también con bases aleatorias (***Figura 20***).

	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
Puerta	→	→	↑	↑	↑	→	→	→	↑	→
Bit	0	1	1	1	0	0	0	1	0	0

Figura 20. Medición de qubits

- Cuando la base de Bob coincide con la de Alice, el bit es correcto.
- Cuando no coincide, el resultado es aleatorio.

Posteriormente, a través de un canal clásico, Alice y Bob comparan las bases utilizadas, sin revelar valores de los bits. Los bits en los que coinciden las bases se conservan, mientras que, los demás se descartan. Por lo que, el resultado final es la clave secreta conocida únicamente por ambos ***(Figura 21)***.

	2	4	5	6	10
Puerta	→	↑	↑	→	→
Bit	1	1	0	0	0

Figura 21. Resultado Protocolo BB84

Esta analogía de la caja y las fichas ilustra cómo BB84 permite a Alice y Bob generar una clave secreta compartida de forma segura. Conforme al principio de incertidumbre de Heisenberg, la seguridad del canal cuántico frente a espías se mantiene efectiva, ya que cualquier intento de observación altera los qubits y puede ser detectado.

La tecnología de distribución cuántica de claves (QKD) ha experimentado un perfeccionamiento constante y, según la empresa *HEQA Security* —referente en el ámbito de la ciberseguridad y proveedora de soluciones en este campo—, se pueden mencionar algunos casos destacados de su aplicación [51]:

- La empresa surcoreana *SK Telecom*, en conjunto con *Samsung*, presentó el *Galaxy Quantum2*, su segundo teléfono inteligente equipado con criptografía cuántica. Este avance se dio tras la exitosa integración de QKD en equipos IP y la culminación del desarrollo de una red privada virtual cuántica (VPN).

- *HD Hyundai Heavy Industries (HHI)* adoptó la criptografía cuántica en sus sistemas de comunicación para resguardar su tecnología de defensa, resaltando que esta innovación se ha vuelto fundamental para la protección de información crítica en el entorno del 5G.

- En Estados Unidos, *Verizon* llevó a cabo una prueba de QKD en Washington D. C., logrando resultados positivos que la colocan entre las primeras operadoras del país en implementar esta tecnología. Este logro se suma a los ensayos previamente efectuados por *Telefónica* y *Huawei*.

2.2.1. VENTAJAS DE LA CRIPTOGRAFÍA CUANTICA

La criptografía clásica y moderna se usan comúnmente, sin embargo, se han tenido ataques poniendo en riesgo la confidencialidad, integridad y disponibilidad de la información ya que como mencionan Sehgal y Gupta [25] entre las limitaciones que presenta son:

- Mayor consumo de energía.
- Mayor producción de calor.
- Saturación de transistores.
- Fácilmente decodificable.
- Procesamiento lento.
- Las operaciones se basan en la multiplicación de números primos, lo cual puede ser fácilmente computado por computadoras cuánticas.

Por lo que avanzar a la siguiente etapa, Sehgal y Gupta [25] aportan un listado de las ventajas del uso de la criptografía cuántica, así como aplicaciones comunes de la criptografía cuántica en el campo de la comunicación, por ejemplo:

- La operación es reversible, es decir, se puede deducir la entrada a partir de la salida.
- No se produce calor, reduciendo la necesidad de sistemas de refrigeración y mejora la eficiencia.
- La disipación de energía es nula.
- Proporciona una estabilidad computacional mejorada.
- Permite la computación paralela, acelerando los procesos.
- Los recursos computacionales, tanto en hardware como en software, se necesitan una cantidad reducida.
- Es accesible para su implementación en infraestructura de comunicación existentes.
- Permite una alta tasa de transmisión de bits.
- Maneja una cadena de bits reducida, optimizando el almacenamiento y la transmisión.

Este tipo de criptografía se ha aplicado en múltiples áreas donde la seguridad y la integridad de la información son esenciales. Entre sus usos más destacados se encuentran:

- Cifrado de datos
- Comunicación digital
- Criptomoneda (Bitcoins)
- Firma digital
- Transacciones comerciales
- Cuántica en el campo de Internet
- Comercio electrónico
- Planes de campaña política
- Red eléctrica
- Votación electoral segura
- Examinando la estructura del ADN y las neuronas

2.3. ALGORITMOS CUANTICOS VS CRIPTOGRAFÍA MODERNA

De acuerdo con la sección anterior se mencionan ciertas limitaciones de la criptografía moderna, misma que se ha considerado segura por muchos años, ya que cuentan con operaciones que requieren un largo periodo de tiempo de resolución para obtener la información por parte de los atacantes, sin embargo, dado el avance tecnológico cuántico se ha demostrado que existen desafíos a la seguridad de los algoritmos clásicos.

Los algoritmos cuánticos tienden a realizar las operaciones con una velocidad exponencialmente alta, sin embargo, se han investigado algunos algoritmos los cuales junto con los criptosistemas clásicos podrían mejorar la seguridad en la información, Bishwas y Advani [1] concluyeron en su investigación que el modelo hibrido de clásico-cuántico tanto con la criptografía simétrica como asimétrica es sólido desde su punto de vista teórico, por lo cual podría resistir a los ataques cuánticos, sin embargo con algunas limitaciones.

Autores como Thamilarasi et al. [21] mencionan el algoritmo Shor no como un criptosistema, sino como la interacción que tiene con la criptografía cuántica sobresaliendo la dualidad en la computación cuántica con los sistemas criptográficos actuales. Ya que al ser un algoritmo Shor un algoritmo que amenaza la seguridad con la criptografía clásica, ofrece un mecanismo de cifrado prácticamente imposible para los algoritmos asimétricos.

De igual manera, Sakhi et al. [10], proponen el algoritmo Grover que ha mostrado una creciente capacidad para resolver problemas en múltiples problemas y escenarios en la criptografía cuántica.

A continuación se explicará el funcionamiento de ambos algoritmos encontrados dentro de la criptografía cuántica.

2.3.1. ALGORITMO SHOR

En 1994, el matemático estadounidense Peter Shor propone el algoritmo Shor (AS), con la cual se podría fácilmente hackear la clave publica cifrada con una computadora cuántica.

El AS busca factorizar grandes números en tiempo polinomial, lo cual afecta a los criptosistemas actuales, como el algoritmo RSA que utiliza una clave publica N formada por la multiplicación de dos números primos grandes; dicha operación es viable para derrotar el cifrado RSA con métodos cuánticos [4].

Wang y Sakk [7] señalan que el funcionamiento del AS reduce la complejidad computacional de un nivel polinomial $O(n^3)$.

Kumar y Thangaraj [4] enlistan los pasos del algoritmo Shor para la factorización de los números enteros, como se describe en seguida:

1. **Elegir un entero positivo (*r*):**
   Seleccionar un número *r* que cumpla con dos condiciones:
   - *r* < *N,* donde N es el número que se quiere factorizar
   - *r y N* son coprimos (es decir, MCD (*r, N) =1*).

2. **Calcular el período *p* de la función $f_r(x) = r^x \bmod N$:**
   Utilizar una computadora cuántica para determinar el período *p*, el periodo de *p* es el menor entero positivo tal que $r^p \equiv 1 \bmod N$

3. **Repetir desde el paso 1 para números impares:**
   Si se encuentra un resultado inválido como números impares, iniciar nuevamente desde el paso 1.

4. **Verificar que *p* sea un número par:**

   Como *p* es un entero par, el valor módulo *N* de $(r^{\frac{p}{2}} - 1)$ $(r^{\frac{p}{2}} + 1)$ será cero para todos los enteros naturales *p*.

5. **Comprobar si $\left(r^{\frac{p}{2}} + 1\right) \equiv 0\ mod\ N$:**

   Si se cumple esta condición, regresar al paso 1, para asegurarse de que la solución sea válida y no contenga factores triviales.

6. **Asegurarse de que $\left(r^{\frac{p}{2}} + 1\right) \neq 0\ mod\ N$:**

   Si $\left(r^{\frac{p}{2}} + 1\right)$ no es cero módulos *N*, continuar al siguiente paso.

7. **Calcular el máximo común divisor para encontrar un factor de** N**:**

   Resolver la ecuación:

$$d_1 = MCD\left(r^{\frac{p}{2}} - 1\right), N$$

$$d_2 = MCD\left(r^{\frac{p}{2}} + 1\right), N$$

   Donde el valor de *d* es un factor no trivial de *N*, completando así la factorización.

Ejemplo, factorizar una clave publica de tamaño *N=21.*

1. Seleccionar el número 10 como *r,* siendo 10 coprimo y menor que 21

$$MCD(10{,}21) = 1$$

2. Calcular *p* con la fórmula $f_r(x) = r^x\ mod\ N$ hasta obtener como resultado 1

$$f(1) = 10^1\ mod\ 21 = 10$$
$$f(2) = 10^2\ mod\ 21 = 16$$
$$f(3) = 10^3\ mod\ 21 = 13$$
$$f(4) = 10^4\ mod\ 21 = 4$$
$$f(5) = 10^5\ mod\ 21 = 19$$
$$f(6) = 10^6\ mod\ 21 = 1$$
$$\therefore p = 6$$

3. Como *6* es un número par, continuar

4. Calcular $(r^{\frac{p}{2}} - 1)\ (r^{\frac{p}{2}} + 1)$

$$\left(r^{\frac{p}{2}} - 1\right) = \left(10^{\frac{6}{2}} - 1\right) = 999$$

$$\left(r^{\frac{p}{2}} - 1\right) = \left(10^{\frac{6}{2}} + 1\right) = 1001$$

$$(999)(1001) \equiv 999999$$

$$999999\ mod\ 21 = 0$$

Como el resultado es igual a 0, se considera un número par.

5. Calcular $\left(r^{\frac{p}{2}} + 1\right) \equiv 0\ mod\ N$

$$10^{\frac{6}{2}} = 1000 + 1$$

$$1001\ mod\ 21 = 14$$

$$1001\ mod\ 21\ \neq 0\ mod\ N$$

Ya que el resultado es diferente a 0, ir al paso 6.

6. Se asegura que $\left(r^{\frac{p}{2}} + 1\right) \neq 0\ mod\ N$

$$\left(10^{\frac{6}{2}} + 1\right)\ mod\ 21 \neq 0$$

$$14 \neq 0$$

7. Se calcula los factores de N

$$d_1 = MCD\left(10^{\frac{6}{2}} - 1\right), N = MCD(13 - 1, 21) = MCD\ (12, 21) = \mathbf{3}$$

$$d_2 = MCD\left(10^{\frac{6}{2}} + 1\right), N = MCD(13 + 1, 21) = MCD\ (14, 21) = \mathbf{7}$$

$$\therefore los\ factores\ encontrados\ son\ 3\ y\ 7$$

Como se observa, multiplicar dos números primos grandes para formar *N* es crucial para la seguridad del criptosistema clásico de RSA, sin embargo, con este algoritmo para descomponer a *N* pone en peligro la seguridad de RSA. La criptografía cuántica y el algoritmo de Shor muestran un nuevo panorama entre los límites del cálculo, la seguridad y la privacidad.

2.3.2. ALGORITMO GROVER

El algoritmo Grover es creado en 1996 desarrollado por Lov Grover. Este algoritmo Zidan et al. lo describe como un proceso que realiza operaciones de búsqueda en bases de datos no ordenadas más rápido que los algoritmos clásicos. Es decir, en tiempo cuadrático en comparación con otros algoritmos cuánticos logra tener mayor velocidad ya que es único por la facilidad de integración como subrutina, estos trabajos refuerzan la mecánica cuántica, así como, las aplicaciones de la computación cuántica [9][21][16].

Al igual que en los sistemas clásicos, es importante tener puertas lógicas cuánticas para el control de los estados; las puertas lógicas son operaciones unitarias que se representan como matrices unitarias y manipulan los estados de los qubits, dos de ellos son [10][22]:

- Hadamard: Es una puerta de un qubit, la cual permite construir estados superpuestos a partir de qubits individuales [10].

$$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

- CNOT: Es una operación de dos qubits donde uno actúa como control y el otro como objetivo [8].

$$CNOT(0,1) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

Suponiendo que se tiene una base de datos no estructurada con *N* elementos (0, *N-1*), con un sistema clásico tendríamos que probar uno por uno, sin embargo, con el algoritmo Grover se necesita $O(\sqrt{N})$ intentos [14][18].

Sakhi et al. [10] enlistan los pasos del algoritmo Grover de la siguiente manera:

1. **Considerar un estado inicial: $|0\rangle^{\otimes n}$:**
   Se inicia con el estado $|0\rangle$. Si se tiene *n* qubits, el estado inicial será el vector $|000\ldots.0\rangle$

2. **Aplicar la puerta Hadamard en los primeros *n* qubits:**
   El estado base $|0\rangle$ se transforma en una superposición de $|0\rangle$ y $|1\rangle$ con la misma probabilidad. De esta manera, se obtienen los posibles casos con cada registro de qubits.

3. **Aplicar el oráculo (función *f*)*:***
   El oráculo es una función que representa una operación cuántica que marca el estado si la entrada o el estado es correcto, de lo contrario, no realiza ningún proceso.
   $f(x) = 1$, estado correcto, y le ponen una fase negativa $|x\rangle$
   $f(x) = 0$, estado incorrecto, y no cambia el signo

4. **Aplicar nuevamente la puerta Hadamard a cada uno de los términos:**
   Con la finalidad de aumentar las probabilidades de medir el estado correcto.

5. **Realizar una medición:**
   Finalmente, se mide el estado del registro, el cual tiene una alta probabilidad de ser la respuesta correcta,

Para ilustrar el proceso del algoritmo, se considera un cifrado simétrico con una clave de 3 bits. Las posibles claves sería 000 a 111, lo que sería $2^3 = 8$ posibles claves.

1. **Considerar un estado inicial: $|0\rangle^{\otimes n}$:**

$$|000\rangle, |001\rangle, |010\rangle, |011\rangle, |100\rangle, |101\rangle, |110\rangle, |111\rangle$$

2. **Aplicar la puerta Hadamard en los primeros *n* qubits:**

$$\frac{1}{\sqrt{8}}(|000\rangle + |001\rangle + |010\rangle + |011\rangle + |100\rangle + |101\rangle + |110\rangle + |111\rangle)$$

3. **Aplicar el oráculo (función *f*):**

Suponiendo que la clave correcta es 010. La función cambiará el signo del estado y lo transformará en

$$\frac{1}{\sqrt{8}}(|000\rangle + |001\rangle - |010\rangle + |011\rangle + |100\rangle + |101\rangle + |110\rangle + |111\rangle)$$

4. **Aplicar nuevamente la puerta Hadamard a cada uno de los términos:**

$$H|000\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |100\rangle)$$
$$H|001\rangle = \frac{1}{\sqrt{2}}(|001\rangle + |101\rangle)$$
$$H|010\rangle = \frac{1}{\sqrt{2}}(|010\rangle + |110\rangle)$$
$$H|011\rangle = \frac{1}{\sqrt{2}}(|011\rangle + |111\rangle)$$

Y así sucesivamente.

5. **Realizar una medición:**

Al realizar en repetidas ocasiones el paso 3 y 4, se logra probar con la clave correcta en el algoritmo, la cual es 010.

2.4. OBSTACULOS

Es evidente que se percibe que la criptografía cuántica es una forma segura de enviar información a través de canales clásicos, haciendo uso de los criptosistemas clásicos. Sin embargo, existen factores que han impedido que se haya implementado como una nueva y única solución para la seguridad de la información [25]:

- No es viable para distancias largas (distancia máxima disponible es de 90 millas).
- Ha afectado el empleo de muchas personas.
- El algoritmo es complejo de implementar.
- El costo inicial es muy alto.
- Dependiente del medio de transmisión.
- Es una técnica punto a punto, por lo que no se puede usar para firmar documentos públicos. Solo es posible la autenticación de mensajes privados.
- La criptografía en luz solar enfrenta muchos desafíos.

De este modo, la criptografía cuántica tiene una práctica mínima, aunque va aumentando y se espera que sea el futuro de la comunicación y las redes. Los criptosistemas modernos son los mayormente utilizados ya que cumplen con el objetivo de la seguridad de la información, (la triada CID), es evidente una vulnerabilidad para los sistemas modernos, puesto que el avance tecnológico permite el ataque con algoritmos cuánticos, por ejemplo el algoritmo RSA. Como se ha mencionado anteriormente con el algoritmo Shor se pueden realizar operaciones grandes, por lo que el tiempo disminuya polinomialmente y esto ha causado inseguridad en los datos cifrados.

Los algoritmos de la criptografía cuántica han traspasado la seguridad de la criptografía clásica y moderna, sin embargo, es evidente que también cuenta con debilidades. Vadakkethil et al. [15], dicen que el uso de la criptografía cuántica también puede llevar a un aumento en la sensación artificial de seguridad, y es que aparenta un método de comunicación altamente eficiente, cuando su único propósito es garantizar la transmisión segura de información. Es claro que considera que no considera diversas vulnerabilidades en la protección comunitaria, por ejemplo, no proporciona defensa contra ataques de ingeniería social o malware.

A pesar de que estos algoritmos cuánticos sean una amenaza para la criptografía clásica, existen barreras que deben tratarse antes de utilizar estos algoritmos cuánticos [6][1]:

1. Requiere una transmisión en tiempo real, ya que los fotones no pueden ser retenidos para cálculos posteriores.
2. En la implementación de redes grandes o distribuidas, es necesario coordinar el procesamiento y transmisión de información.
3. Carece de mecanismos para sustituir las firmas digitales, esenciales para la autenticación e integridad de los datos.
4. Necesita precisar los dispositivos utilizados y la escalabilidad de la infraestructura desde el punto de vista de las implementaciones, además, actualmente es costosa e inaccesible.

Conforme al algoritmo Shor, de acuerdo con Kumari et al. [12] presentan algunos desafíos como la corrección de errores, los efectos de ruido y la decoherencia hacen que sea propenso a cometer errores. Así mismo, la escalabilidad es otro reto, ya que actualmente el número de qubits que los sistemas cuánticos pueden soportar es limitado.

Por otro lado, el algoritmo Grover no pueda romper con la criptografía de clave publica, reduce el tiempo para un ataque de fuerza bruta.

A manera de resumen en la ***Tabla 16***, muestra algunos obstáculos encontrados de los algoritmos cuánticos ante los criptosistemas modernos:

Algoritmo	**Shor**	**Grover**
Tecnología	Óptica integrada	RMN (Resonancia Magnética Nuclear)
Criptosistema clásico	RSA	AES, SHA
Problema que resuelve	Factorización de números primos	Búsqueda no estructurada
Tiempo	Polinómico, exponencialmente en método clásico	Cuadrático
Obstáculos	- Requiere una computadora cuántica estable con suficientes qubits. - Escalabilidad limitada - Corrección de errores cuánticos	- Aplica solo a problemas no estructurados. - No supera significativamente los sistemas actuales. - Beneficio marginal frente a claves largas. - Corrección de errores compleja.

Tabla 16. Comparación entre algoritmos cuánticos que atacan a los criptosistemas

2.5. RESUMEN

El desarrollo de la computación cuántica ha cambiado el panorama de la seguridad informática. Algoritmos como Shor y Grover han demostrado que los sistemas criptográficos modernos pueden ser vulnerables ante el poder de procesamiento de las computadoras cuánticas. Ante esta situación, la ciberseguridad cuántica surge como un campo en crecimiento que busca mitigar estos riesgos mediante nuevas técnicas y protocolos.

En este capítulo se ha analizado el impacto de la computación cuántica en la seguridad de la información, destacando los algoritmos cuánticos que pueden comprometer la criptografía tradicional. También se han explorado las soluciones que ofrece la criptografía cuántica y los desafíos que enfrenta para su adopción.

Dos de los algoritmos cuánticos más relevantes en este contexto son Shor y Grover, cuyos efectos en la seguridad digital se resumen en la ***Tabla 17***.

Algoritmo	**Impacto potencial**
Shor	- Podría comprometer sistemas que protegen infraestructuras críticas, por ejemplo, redes de energía, telecomunicaciones y sistemas gubernamentales. - Destruiría la confianza en la mayoría de las comunicaciones seguras en la web actual.
Grover	- Reduciría la seguridad efectiva de claves simétricas (AES) y funciones hash (SHA). - Obliga a usar claves más largas, aumentando la carga computacional.

Tabla 17. Impacto potencial en la criptografía clásica

Dado el avance acelerado en este campo, resulta crucial examinar las tendencias actuales y futuras en ciberseguridad cuántica. En el siguiente capítulo, se abordarán las estrategias post-cuánticas y las innovaciones en seguridad que buscan hacer frente a esta nueva era tecnológica.

CAPÍTULO III. TENDENCIAS EN LA CIBERSEGURIDAD CUÁNTICA

En este capítulo, se estudiarán las tendencias emergentes en ciberseguridad cuántica, incluyendo un algoritmo post-cuántico y los enfoques que actualmente se investigan para fortalecer la protección de la información.

3.1. POST-CUÁNTICA

A medida que la computación cuántica avanza, es imprescindible desarrollar mecanismos de protección que puedan resistir sus capacidades de procesamiento. La criptografía post-cuántica se perfila como una de las principales soluciones para garantizar la seguridad en un mundo donde los ataques cuánticos sean viables.

La computación cuántica al igual que la computación clásica manifiestan retos es por lo que a medida que persiste la labor de desarrollar computadoras cuánticas prácticas, el sector de ciberseguridad debe prepararse para la era post-cuántica [12], puesto que puede implicar desarrollar nuevos algoritmos de cifrados antes ataques cuánticos como se explicó en el capítulo pasado.

De acuerdo con Hegde et al. [18], la criptografía post-cuántica buscar crear sistemas criptográficos que puedan resistir ataques de computadoras cuánticas usando problemas matemáticos considerados difíciles de resolver para computadoras tanto clásicas como cuánticas.

Del mismo modo Govindhan y Kumar [37] definen criptografía post-cuántica como un subconjunto del procesamiento cuántico enfocado a la seguridad y la autenticación de datos, misma que necesita de trabajo de investigación y reflexión.

Lu et al. [23] de igual forma que Hegde [18] definen la criptografía post-cuántica, como un algoritmo criptográfico desarrollado para abordar las amenazas de seguridad en la era de las computadoras cuánticas, estos algoritmos pueden superar la velocidad de computación de los sistemas criptográficos de clave pública existentes, manteniendo un nivel de seguridad equivalente.

Lella et al. [16] señalan de acuerdo con el tipo de problema computacional, podemos distinguir las siguientes cuatro categorías principales de algoritmos de criptografía post-cuántica (PQC):

- **Basados en códigos:** esquemas de firma y cifrado basados en la dificultad de problemas de teoría de códigos como la decodificación de síndrome y la decodificación acotada de Goppa.
- **Basados en redes (látices):** esquemas de firma y cifrado basados en problemas de teoría de redes como el problema del vector más corto (SVP) y el aprendizaje con error (LWE).
- **Basados en hash:** esquemas de firma construidos utilizando funciones hash criptográficas, por ejemplo, XMSS y SPHINCS.
- **Multivariable:** esquemas de firma y cifrado basados en polinomios multivariados y la dificultad de resolver un problema lineal, por ejemplo, Rainbow y UOV.

Aldeco y Aguilar [48] presentan retos asociados a estas categorías:

- **Basada en códigos**: utiliza códigos difíciles de descifrar. Su principal desafío es el gran tamaño de las claves públicas, por lo que la investigación se centra en reducirlas y en desarrollar protocolos eficientes. Se considera una de las alternativas más prometedoras frente a ataques cuánticos.

- **Multivariable:** La principal ventaja de este criptosistema es que las firmas que genera son mucho más pequeñas que las de otros esquemas post-cuánticos. La entidad que firma puede hacerlo de manera eficiente gracias a una estructura especial que facilita la generación de la firma en un tiempo razonable. Aunque un atacante podría intentar descubrir esta estructura, hasta ahora no existe ningún método que lo haga de forma efectiva, por lo que sigue considerándose un problema difícil de resolver.

De igual manera, Bermúdez [50] menciona aplicaciones de las distintas categorías:

- **Basados en códigos:** *NTRU* relevante en aplicaciones donde la velocidad y la eficiencia son críticas; y *Learning With Errors (LWE)* permite ser utilizado en aplicaciones criptográficas, incluyendo cifrado, firmas digitales y esquemas de intercambio de llaves.
- **Basados en redes (látices):** *McEliece*, primordial en comunicaciones gubernamentales y militares; y *LDPC y códigos polares* se utilizan en comunicaciones modernas.
- **Basados en hash:** Las funciones hash son fundamentales desde firmas digitales hasta la integridad de los datos.

Así mismo, en Bermudez [50], se comparte una tabla comparativa **(Tabla 18)**

Enfoque	Descripción	Ventajas	Desventajas
Criptografía basada en retículas	Utiliza problemas geométricos difíciles como el problema del vector más corto.	Alta seguridad y flexibilidad, adecuado para múltiples aplicaciones.	Claves más grandes, mayor complejidad computacional.
Criptografía basada en códigos	Se basa en problemas de decodificación de códigos, como los códigos Goppa.	Probado con el tiempo, altamente seguro frente a ataques cuánticos.	Claves públicas grandes, menos eficiente en ciertas aplicaciones.
Funciones hash	Emplea funciones hash resistentes a colisiones para crear firmas y cifrados.	Resistente a ataques cuánticos, paralelizable y eficiente.	No tan flexible como otros enfoques para ciertas aplicaciones.

Tabla 18. Comparación de Enfoques de Criptografía Post-Cuántica [50]

3.2. ALGORTIMO POST-CUANTICO

Lella [16] refiere que se han encontrados proyectos y bibliotecas donde implementan esquemas post-cuánticos por ejemplo: Codecrypt, Open Quantum Safe, Java Lattice-based Cryptography Library, Microsoft's Lattice Cryptography Library, CRYSTALS y libPQP.

Ristov y Koceski [38] refiere que NIST (Instituto Nacional de Estándares y Tecnología) publicó un artículo, el 5 de julio de 2022, anunciando los primeros cuatro algoritmos de criptografía post-cuántica (PQC). Así mismo, el Mecanismo de Encapsulación de Claves (KEM) de la Suite Criptográfica para Redes Algebraicas CRYSTALS-Kyber fue el único aprobado, algoritmo basado en redes (látices).

Kyber es un mecanismo de encapsulación de claves seguro bajo ataque de cifrado elegido indistinguible (IND-CCA2), cuya seguridad se basa en la dificultad de resolver el problema de aprendizaje con errores (LWE) sobre redes modulares. Kyber se presenta en tres niveles diferentes de seguridad, que han sido probados y tienen diferentes objetivos. Kyber-512 tiene como objetivo una seguridad equivalente a AES-128, Kyber-768 a la del AES-192 y Kyber-1024 a la del AES-256 [26].

Los criptosistemas cumplían con el objetivo de la seguridad de la información, la triada CID, pero con el avance tecnológico mostró debilidades de las amenazas que surgen a raíz de la computación cuántica. Por ejemplo, el algoritmo RSA (Rivest-Shamir-Adleman), uno de los primeros sistemas de criptografía de clave pública y ampliamente utilizado para la seguridad de datos, se basa en la dificultad de factorizar el producto de dos números primos grandes [3]. Sin embargo, como se ha mencionado anteriormente, con el algoritmo Shor se puede realizar operaciones grandes, por lo que el tiempo disminuye polinomialmente.

A la fecha, grandes cantidades de datos se cifran, se transmiten y se almacenan buscando asegurar la confidencialidad de la información, como se menciona anteriormente, las computadoras cuánticas representan una amenaza a los algoritmos cuánticos tanto para claves publicas asimétricas (RSA) como para algoritmos de clave simétrica (DES, 3DES, AES).

Por lo que, los investigadores han trabajado para asegurar que los datos estén seguros y prevenir las amenazas cuánticas, surgiendo los algoritmos post-cuánticos como BB84 (mencionado en el capítulo 2) y CRYSTALS-Kyber. Estas propuestas matemáticas muestran una promesa ante ataques cuánticos, como algoritmo Shor y el algoritmo Grover, no solo desde un punto de vista teórico, sino que también para la protección de la información.

3.3. DESAFIOS

Según autores como Bermudez [50], se menciona que la transición hacia la criptografía post-cuántica presenta varios desafíos relacionados con eficiencia, compatibilidad y estándares.

- ***Eficiencia y rendimiento:*** Muchos algoritmos post-cuánticos requieren claves más grandes y operaciones más complejas que los algoritmos clásicos, lo que puede afectar la velocidad y el rendimiento. Por ejemplo, los esquemas basados en retículas, aunque seguros, son más pesados que el RSA.

    - *Impacto en dispositivos de bajo consumo:* Dispositivos *IoT* y sistemas embebidos, con recursos limitados, pueden tener dificultades para implementar estos algoritmos, lo que puede requerir versiones optimizadas o soluciones híbridas que combinen criptografía clásica y post-cuántica.

- *Optimización de algoritmos:* La investigación busca reducir el tamaño de las claves, mejorar la velocidad de operaciones y adaptar los algoritmos para hardware especializado.

- ***Compatibilidad y transición:*** La infraestructura global está basada en algoritmos clásicos, por lo que adoptar nuevos algoritmos implica actualizaciones masivas.

    - *Soluciones híbridas:* Durante la transición, se usarán combinaciones de algoritmos clásicos y post-cuánticos para mantener compatibilidad.

    - *Migración de sistemas críticos:* Infraestructuras financieras y gubernamentales requieren planificación cuidadosa, evaluación de riesgos y capacitación del personal para la implementación segura de algoritmos post-cuánticos.

- ***Estándares y regulaciones:*** El desarrollo de estándares y regulaciones es crucial para garantizar que los algoritmos sean seguros y eficientes.

    - *Papel de organizaciones internacionales:* ISO y NIST serán clave en la creación de estándares adoptados por gobiernos y empresas, facilitando la transición.

    - *Cumplimiento regulatorio:* Las regulaciones definirán los requisitos de adopción en sectores financieros, sanitarios y gubernamentales, asegurando una implementación segura y oportuna.

3.4. RESUMEN

El desarrollo de la ciberseguridad cuántica y la criptografía post-cuántica representan un paso fundamental en la protección de la información ante amenazas futuras.

Si bien todavía existen desafíos técnicos y prácticos, tales como la eficiencia y el rendimiento, especialmente en dispositivos *IoT* y sistemas embebidos; la compatibilidad con sistemas existentes, que puede requerir soluciones híbridas; y la necesidad de estándares y regulaciones, con la participación de organismos como NIST e ISO, las investigaciones actuales están sentando las bases para un entorno digital más seguro en la era de la computación cuántica.

Con esto, se concluye el análisis de la evolución de la criptografía y la seguridad de los datos, resaltando la necesidad de continuar explorando nuevas soluciones que garanticen la confidencialidad y la integridad de la información en el futuro.

CONCLUSIÓN

En conclusión, se ha cumplido el objetivo general de la tesina, puesto que se ha documentado la importancia de la seguridad de los datos en una organización ante algoritmos cuánticos, para comprender su origen y evolución a las tendencias futuras.

La ciberseguridad ha evolucionado en diferentes etapas, desde los métodos clásicos hasta las soluciones más avanzadas propuestas por la criptografía cuántica y post-cuántica. La criptografía clásica y moderna han sido fundamentales para proteger la información, pero con el advenimiento de la computación cuántica, surgen nuevos desafíos que amenazan la seguridad de los sistemas actuales.

Los algoritmos cuánticos, como el de Shor y Grover, tienen el potencial de debilitar significativamente la seguridad de los sistemas utilizados hoy en día. Ante esta nueva realidad, la criptografía cuántica emerge como una respuesta prometedora, proporcionando soluciones como la distribución cuántica de claves (QKD), que se basa en principios físicos para ofrecer una seguridad más robusta que la de los métodos tradicionales.

A pesar de las promesas de la criptografía cuántica, todavía existen limitaciones, tanto tecnológicas como de infraestructura, que dificultan su implementación a gran escala. Es aquí donde la criptografía post-cuántica juega un papel clave, proporcionando algoritmos diseñados para resistir los ataques de las computadoras cuánticas sin depender de las propias tecnologías cuánticas. Esto abre la puerta a una transición hacia soluciones más seguras, pero también exige tiempo y una integración cuidadosa con los sistemas actuales.

En este contexto, la implementación de un sistema completo de establecimiento de claves híbrido que integre tres métodos diferentes basados en criptografía moderna, criptografía post-cuántica (PQC) y distribución cuántica de claves (QKD) puede ser adecuada para conexiones de alta velocidad entre pares que requieren garantías de alta seguridad, como entre entidades gubernamentales, instituciones de seguridad, nodos de infraestructura crítica, centros de datos, operadores de telecomunicaciones, proveedores de servicios en la nube o en el sector financiero.

El principal beneficio del sistema híbrido propuesto es su alta resistencia a tres tipos de ataques. Los atacantes deben romper tres métodos diferentes (es decir, criptografía pre y post-cuántica, y criptografía cuántica). Específicamente, mientras uno de los métodos de generación de claves permanezca sin ser roto, el combinador de 3 claves es seguro ante ataques de elección adaptativa (IND-CCA) [19].

Dado que los algoritmos cuánticos todavía enfrentan obstáculos que limitan su efectividad total, la criptografía moderna continuará siendo la técnica predominante en la protección de datos. A medida que la tecnología cuántica avance, es probable que los sistemas híbridos basados en criptografía clásica, post-cuántica y cuántica se conviertan en clave para garantizar la seguridad de la información en un entorno cada vez más vulnerable a los ataques cuánticos.

GLOSARIO

AES (Advanced Encruption Standard)	Algoritmo de cifrado de clave simétrica y que cifra por bloques [32].
Bit	Unidad de medida de información equivalente a la elección entre dos posibilidades igualmente probables [40].
BB84	Es una forma revolucionaria de codificar información utilizando estados cuánticos ortogonales [22].
Canal cuántico	El canal cuántico es la ruta inalámbrica óptica LOS que se utiliza para transmitir fotones de polarización [39].
CIA/CID	Por sus siglas Confidencialidad, Integridad y Accesibilidad/Disponibilidad
Cifrado	Procedimiento que convierte un mensaje de texto plano en un texto cifrado [41].
Cifrado por bloques	Procesa la entrada en bloques de elementos, produciendo un bloque de salida por cada bloque de entrada [47].
Cifrado por flujo	Procesa los elementos de entrada de manera continua, generando la salida elemento por elemento a medida que se procesa [47].
Confidencialidad	La confidencialidad de los datos e información se materializa en ofrecer acceso a ellos solo a personas autorizadas [24].
Criptografía	Técnica fundamental y eficaz para la transmisión confiable de datos convirtiendo el texto plano en datos cifrados [11].

Criptografía asimétrica	Implica el uso de pares de claves para el cifrado. El par de claves consta de una clave privada conocida solo por el remitente o receptor, y una clave pública compartida públicamente [18].
Criptografía post-cuántica	Es un tipo de criptografía que es resistente a los ataques de los ordenadores cuánticos. Puede utilizarse para proteger los datos y las comunicaciones de ser interceptados y descifrados por los ordenadores cuánticos [29].
Criptografía simétrica	Este tipo de criptografía se utiliza la misma clave en el emisor para cifrar y en el receptor para el descifrado de los datos [11].
Decoherencia	Los estados cuánticos una vez que medimos el estado al interactuar con él, todo el sistema cuántico colapsará a un solo estado con un valor clásico. No se puede medir múltiples estados cuánticos simultáneamente [1].
DES (Data Encryption Standard)	Es un algoritmo de cifrado simétrico por bloques (la información a cifrar se divide en bloques y se aplica el algoritmo a cada uno de ellos) [30].
Disponibilidad	La disponibilidad o accesibilidad se refiere a garantizar el acceso a los datos e información, para los usuarios autorizados, en cualquier momento [24].
Distribución Cuántica de Claves	Es una técnica avanzada que utiliza las propiedades únicas de la física cuántica, como el teorema de no clonación, el principio de incertidumbre de Heisenberg y el entrelazamiento [22].

Entrelazamiento	Es un concepto en la mecánica cuántica en el que dos o más partículas están conectadas de tal manera que el estado de una partícula impacta el estado de la(s) otra(s) instantáneamente, sin importar la distancia entre ellas [22].
Firma digital	Valor calculado mediante un algoritmo criptográfico y asociado a un objeto de datos de tal forma que cualquier receptor de esos datos puede utilizarla para verificar su origen y su integridad [47].
Fotón	Partícula cuántica elemental, sin masa, encargada de transportar la energía electromagnética entre partículas con carga eléctrica [44].
Fuerza bruta	Es un método de piratería informática que utiliza pruebas y errores para descifrar contraseñas, credenciales de inicio de sesión y claves de cifrado [43].
Función hash	Una función hash convierte una cantidad variable de texto en un valor pequeño de longitud fija llamado valor hash, código hash o resumen, cuenta con propiedades adicionales que la hacen útil como parte de otro algoritmo criptográfico, como un código de autenticación de mensajes (MAC) o una firma digital. [47]
GF (2^n)	Los cuerpos finitos de orden 2^n son llamados cuerpos binarios o cuerpos finitos de característica dos. Son interesantes porque son particularmente eficientes para la implementación en hardware o en ordenadores binarios [32].

Grover	El algoritmo de Grover aprovecha la interferencia cuántica para buscar de manera eficiente en una base de datos no ordenada [18].
Hash	Transforman los mensajes o datos de entrada de cualquier longitud en salidas de longitud fija llamadas valores hash [18].
Integridad	La integridad de los datos e información significa que deben mantenerse en su forma correcta y completa y no deben modificarse sin autorización, ya sea accidentalmente o de manera intencionada [24].
Látices	Conjunto parcialmente ordenado en el cual dos elementos cualesquiera tienen un único límite superior mínimo y un único límite inferior máximo [].
MAC	Elemento de datos asociado a un bloque de información o mensaje, generado mediante una transformación criptográfica que involucra una clave secreta y, típicamente, una función hash criptográfica del mensaje [47].
No clonación	Este teorema establece que los estados cuánticos no pueden ser copiados, una vez que interactúan con el sistema, la superposición colapsará en un solo estado [1].
Polarización	Es la propiedad de ciertos tipos de ondas que describe la orientación de sus oscilaciones. Cuando una onda vibra en una sola dirección, podemos decir que está polarizada linealmente en esa dirección [45].

Principio de incertidumbre Heisenberg	Asegura que es imposible determinar, con precisión absoluta y de forma simultánea, el valor de dos magnitudes conjugadas de un sistema elemental [36].
Qubit	La unidad mínima de información cuántica es el qubits (quantum bit por sus siglas en inglés) [5].
Semi -primo	Un número natural se denomina semiprimo si es igual al producto de dos números primos, que pueden ser iguales o distintos [53].
Shor	El algoritmo de Shor factoriza enteros de manera eficiente, lo que representa un desafío significativo para la criptografía clásica de clave pública, que depende de problemas computacionalmente difíciles como los logaritmos discretos y la factorización de enteros [18].
Suma de comprobación	Es una función matemática que comprueba los archivos en busca de daños antes de guardarlos [42].
Superposición	La superposición, denota la capacidad de un sistema cuántico, como un qubit en la computación cuántica, de ocupar múltiples estados simultáneamente [22].
S-cajas	Son unas tablas en las que se encuentra el valor inverso de cada elemento de GF (2^8) en valor hexadecimal multiplicado por una matriz constante y sumado un vector constante, cada byte al tratarse de 8 elementos que pueden ser o 0 o 1 entonces se tratan de elementos de GF (2^8) [31].
Sustitución	Cada elemento del texto plano (bit, letra o grupo de bits o letras) se asigna a otro elemento [47].

Transposición	Los elementos del texto plano se reorganizan. El requisito fundamental es que ninguna información se pierda (es decir, que todas las operaciones sean reversibles) [47].

REFERENCIAS

[1] K. Bishwas y J. Advani, «Managing Cyber Security with Quantum Techniques», 2021 International Conference On Electrical, Computer And Energy Technologies (ICECET), vol. 20, pp. 1-7, dic. 2021, doi: 10.1109/icecet52533.2021.9698591.

[2] M. A. M. Vilchis, R. S. Ortigoza, y E. B. Molina, «Criptografía cuántica: un nuevo paradigma», Polibits, vol. 36, pp. 30-35, jul. 2007, doi: 10.17562/pb-36-6.

[3] D. Silva y R. Núñez, «Exploración de las posibilidades de la computación cuántica para la criptografía», Ciencia Inteligente, vol. 1, n.o 2, nov. 2023, [En línea]. Disponible en: https://cienciainteligente.com/index.php/CIN/article/view/16/16

[4] K. A. Kumar and S. J. J. Thangaraj, «Improving Quantum Computer's Error Rate Using Quantity Computational Algorithm Comparing with Shor's Algorithm», 2024 International Conference on Advances in Data Engineering and Intelligent Computing Systems (ADICS), Apr. 2024, doi: 10.1109/adics58448.2024.10533506.

[5] R. Lema Andrango, «Estudio Introductorio a la Criptografía Cuántica», Trabajo de Integración Curricular, Escuela Politécnica Nacional, Facultad de Ingeniería Eléctrica y Electrónica, Director: W. F. Flores Cifuentes, Quito, Ecuador, Sep. 2022.

[6] S. K. Sehgal and R. Gupta, «Quantum Cryptography and Quantum Key, » 2021 International Conference on Industrial Electronics Research and Applications (ICIERA), 2021, doi: 10.1109/ICIERA53202.2021.9726722.

[7] S. P. Wang y E. Sakk, «Quantum Algorithms: Overviews, Foundations, and Speedups», 2021 IEEE 5th International Conference On Cryptography, Security And Privacy, ene. 2021, doi: 10.1109/csp51677.2021.9357505.

[8] R. Huang, X. Tan, and Q. Xu, «Learning to learn variational quantum Algorithm, » IEEE Transactions on Neural Networks and Learning Systems, vol. 34, no. 11, pp. 8430–8440, Feb. 2022, doi: 10.1109/tnnls.2022.3151127.

[9] M. Zidan, A. M. Eisa, M. Qasymeh, and M. a. I. Shoman, «A quantum algorithm for system specifications verification, » IEEE Internet of Things Journal, vol. 11, no. 14, pp. 24775–24794, Mar. 2024, doi: 10.1109/jiot.2024.3383034.

[10] Z. Sakhi, R. Kabil, A. Tragha, and M. Bennai, «Quantum cryptography based on Grover's algorithm, » Second International Conference on the Innovative Computing Technology (INTECH 2012), Sep. 2012, doi: 10.1109/intech.2012.6457788.

[11] M. Ghute y Y. Suryawanshi, «Comparison of Cryptographic Techniques: Classical, Quantum and Neural», 2022 6th International Conference On Electronics, Communication And Aerospace Technology, dic. 2022, doi: 10.1109/iceca55336.2022.10009164.

[12] D. Kumari, A. Namburi, K. Tanuj, R. Rangu, N. K. M. Naidu, y M. Mahmoud, «Quantum Computing in cryptography», 2023 International Conference On Computational Science And Computational Intelligence (CSCI), dic. 2023, doi: 10.1109/csci62032.2023.00086.

[13] M. Ati, «Implementation of quantum cryptography for securing IoT devices», 2023 International Conference On Electrical, Communication And Computer Engineering (ICECCE), dic. 2023, doi: 10.1109/icecce61019.2023.10442918.

[14] S. P. Sanon, I. Alzalam, y H. D. Schotten, «Quantum and Post-Quantum security in future networks», 2023 IEEE Future Networks World Forum (FNWF), vol. 4244, pp. 1-6, nov. 2023, doi: 10.1109/fnwf58287.2023.10520624.

[15] S. E. V. S. Pillai y K. Polimetla, «Analyzing the Impact of Quantum Cryptography on Network Security», 2024 International Conference On Integrated Circuits And Communication Systems (ICICACS), feb. 2024, doi: 10.1109/icicacs60521.2024.10498417.

[16] E. Lella et al., «Cryptography in the Quantum Era», 2022 IEEE 15th Workshop On Low Temperature Electronics (WOLTE), jun. 2022, doi: 10.1109/wolte55422.2022.9882585.

[17] T. Hasija, K. R. Ramkumar, B. Singh, A. Kaur, y S. K. Mittal, «Symmetric Key Cryptography: Review, algorithmic insights, and challenges in the era of Quantum Computers», 2023 14th International Conference On Computing Communication And Networking Technologies (ICCCNT), jul. 2023, doi: 10.1109/icccnt56998.2023.10307081.

[18] S. B. Hegde, A. Jamuar, y R. Kulkarni, «Post quantum implications on private and public key cryptography», 2023 International Conference On Smart Systems For Applications In Electrical Sciences (ICSSES), jul. 2023, doi: 10.1109/icsses58299.2023.10199503.

[19] S. Ricci, P. Dobias, L. Malina, J. Hajny, y P. Jedlicka, «Hybrid Keys in Practice: Combining Classical, Quantum and Post-Quantum Cryptography», IEEE Access, p. 1, ene. 2024, doi: 10.1109/access.2024.3364520.

[20] G. Murali and R. S. Prasad, «Comparison of cryptographic algorithms in cloud and local environment using quantum cryptography, » International Conference on Energy, Communication, Data Analytics and Soft Computing, 2016, doi: 10.1109/icecds.2017.8390165.

[21] V. Thamilarasi, P. K. Naik, I. Sharma, V. Porkodi, M. Sivaram, and M. Lawanyashri, «Quantum computing - navigating the frontier with SHOR's algorithm and quantum cryptography, » International Conference on Trends in Quantum Computing and Emerging Business Technologies CHRIST, vol. 8, pp. 1–5, Mar. 2024, doi: 10.1109/tqcebt59414.2024.10545283.

[22] S. Soumya and T. Chithralekha, "Securing the Quantum Future: Evaluating and standardizing quantum encryption algorithms," 2022 13th International Conference on Computing Communication and Networking Technologies (ICCCNT), pp. 1–8, Jun. 2024, doi: 10.1109/icccnt61001.2024.10724027.

[23] Y. Lu, L. Wei, W. Wu, and Y. Zhang, "Research on Quantum SSL based on national cryptography," The 9th International Conference on Computer and Communication Systems, Apr. 2024, doi: 10.1109/icccs61882.2024.10603232.

[24] D. Popescul, «The confidentiality – integrity – accessibility triad into the knowledge security: a reassessment from the point of view of the knowledge contribution to innovation», SSRN Electronic Journal, jun. 2011, [En línea]. Disponible en: https://papers.ssrn.com/sol3/Delivery.cfm/SSRN_ID2343019_code634928.pdf ?abstractid=2343019&mirid=5

[25] S. K. Sehgal y R. Gupta, «A Comparative Study of Classical and Quantum Cryptography», International Conference On Computing For Sustainable Global Development, mar. 2019, [En línea]. Disponible en: http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=8991298

[26] M. S. Win and T. T. Khin, «Analysis of Quantum Key Distribution Protocols, » IEEE Conference on Computer Applications (ICCA), vol. 2, pp. 357–362, Feb. 2023, doi: 10.1109/icca51723.2023.10181682.

[27] Suetonio & José David Castro de Castro. (2018). «*Vidas de los Césares*». Alianza Editorial.

[28] J. Moazzam, R. Pawar, and M. D. Khare, «Evolution and Advancement of Quantum Computing in the Era of Networking and Cryptography, » 2023 International Conference on Advances in Computation, Communication and Information Technology (ICAICCIT), pp. 817–821, Nov. 2023, doi: 10.1109/icaiccit60255.2023.10465946.

[29] K. Dey, C. Chaudhary, and B. K. A, «Future-Ready Security in the Cloud with Post-Quantum Encryption, » 2023 International Conference on Power Energy, Environment & Intelligent Control (PEEIC), pp. 768–772, Dec. 2023, doi: 10.1109/peeic59336.2023.10450301.

[30] M. G. Larragan, «Criptografía (XLIX): el algoritmo DES (I),» Feb. 26, 2017. https://mikelgarcialarragan.blogspot.com/2017/02/criptografia-xlix-el-algoritmo-des-i.html

[31] L. X. Ahumada-Urquijo, J. Valencia-Ortiz, M. F. Velandia-Beltran, y J. B. Mendoza-Calderón, «Propuestas de mejora DES y Triple DES a lo largo de su historia», Rev. Vínculos, vol. 19, n.º 2, dic. 2022.

[32] J. Martínez De La Torre, «Cifrado de clave privada: AES,» Estancia en Practicas y Proyecto Final de Grado, Universitat Jaume, 2016.

[33] «Algoritmo de criptografía RSA,» Huawei, 2022. https://forum.huawei.com/enterprise/es/algoritmo-de-criptograf%C3%ADa-rsa/thread/691222638527135744-667212881550258176

[34] I. Pedone, A. Atzeni, D. Canavese, and A. Lioy, «Toward a complete software stack to integrate quantum key distribution in a cloud environment, » IEEE Access, vol. 9, pp. 115270–115291, Jan. 2021, doi: 10.1109/access.2021.3102313.

[35] M. S. Rahman and M. Hossam-E-Haider, «Quantum IoT: A quantum approach in IoT security maintenance, » 2019 International Conference on Robotics,Electrical and Signal Processing Techniques (ICREST), pp. 269–272, Jan. 2019, doi: 10.1109/icrest.2019.8644342.

[36] J. Pradilla, «Amplification of the bit rate for quantum key distribution based on cryptographic hash functions, » Optica Pura Y Aplicada, vol. 46, no. 4, pp. 337–343, Dec. 2013, doi: 10.7149/opa.46.4.337.

[37] P. Govindhan y K. Kumar, «Post-quantum cryptography for multiple high-resolution millimeter wave images for enhanced security in IOT networks», 2024 2nd International Conference On Advancement In Computation & Computer Technologies (InCACCT), pp. 529-533, may 2024, doi: 10.1109/incacct61598.2024.10550966.

[38] R. Ristov y S. Koceski, «Quantum resilient public key cryptography in internet of things», 2023 12th MEDITERRANEAN CONFERENCE ON EMBEDDED COMPUTING, vol. 2016, pp. 1-4, jun. 2023, doi: 10.1109/meco58584.2023.10154994.

[39] C. Jenila and R. K. Jeyachitra, «Green indoor optical wireless communication systems: Pathway towards pervasive deployment, » Digital Communications and Networks, vol. 7, no. 3, pp. 410–444, Sep. 2020, doi: 10.1016/j.dcan.2020.09.004.

[40] Real Academia Española. https://www.rae.es/

[41] «¿Qué es la criptografía? - Explicación sobre la criptografía - AWS,» Amazon Web Services, Inc. https://aws.amazon.com/es/what-is/cryptography/

[42] Ciberseg, «¿Qué es una suma de comprobación y cómo se usa?,» Ciberseguridad, Apr. 12, 2022. https://ciberseguridad.com/guias/prevencion-proteccion/suma-comprobacion/

[43] «¿Qué es un ataque de fuerza bruta? | Tipos y cómo funciona| Fortinet,» Fortinet. https://www.fortinet.com/lat/resources/cyberglossary/brute-force-attack

[44] A. M. Ortiz, «Luz: los fotones que se ven y los que no se ven,» The Conversation. https://theconversation.com/luz-los-fotones-que-se-ven-y-los-que-no-se-ven-229034

[45] «Polarización de la luz.» https://www.uv.es/uvweb/fisica/es/catalogo-demos/optica/polarizacion-luz-1286053998317/DemoExp.html?id=1286110847123

[46] «Advanced Encryption Standard (AES)» Jan. 2001. doi: 10.6028/nist.fips.197.

[47] W. Stallings, «Cryptography and Network Security: Principles and Practice», Global Edition. Pearson Educ., Limited, 2022.

[48] R. Aldeco y G. Aguilar, «Introducción a la ciberseguridad y sus aplicaciones en méxico.» Acad. Comput., A. C., 2020.

[49] Teleco Renta. «Teleco Renta | Lemnismath | Protocolo cuántico BB84.» (4 de noviembre de 2024). Accedido el 20 de agosto de 2025. [Video en línea]. Disponible: https://www.youtube.com/watch?v=koJGMOJ7X1I

[50] A. Bermudez, «Criptografía Post-Cuántica: Desafíos y Oportunidades», Repos. Universad Int. SAn Isidro Lbrador, agosto de 2024. [En línea]. Disponible: https://uisil.net/repositorio/articulo/47

[51] H. Security, “Quantum Cryptography in real-world Applications | HEQA Security,” HEQA Security, Aug. 11, 2023. https://heqa-sec.com/blog/quantum-cryptography-in-real-world-applications/

[52] C. L. Liu, Elementos de Matemáticas Discretas (2a.ed.). MCGRAW HILL, 1993.

[53] G. H. Hardy y E. M. Wright, An Introduction to the Theory of Numbers, 6ª ed. Oxford: Clarendon Press, 2008.