Simulación de una comunicación segura mediante criptografía cuántica usando el Protocolo BB84 y el cifrado de Vernam

Universidad Nacional de Ingeniería - Facultad de Ciencias

Profesores

Ronald Jesús Mas Huaman

Angel Enrique Ramirez Gutierrez

Integrantes

Julissa Alisson Garcia Cayetano, 20194100K

David Ademir Sanchez Cotrado, 20190591J

Piero Ayrton Estrada Cántaro, 20190114G

José Gabriel Caycho Villalobos, 20190584C

Resumen

El presente trabajo busca dar a conocer la importancia y la funcionalidad del protocolo BB84 junto con el Cifrado de Vernam en el área de la Criptografía Cuántica. Primero, veremos el marco teórico donde abordaremos temas de Física Cuántica como Principio de la Superposición, Entrelazamiento Cuántico, así como qué son los bits y qubits, entre otros. Estos conceptos nos ayudarán a entender mejor las fases de la encriptación cuántica. Por último, a modo de ejemplo, simularemos el protocolo BB84 y el Cifrado de Vernam, los cuales nos servirán en la encriptación de un mensaje.

Palabras Clave: *Física Cuántica, Criptografía Cuántica, Entrelazamiento Cuántico, Principio de Superposición, Bits, Qubits, Cifrado de Vernam, Protocolo BB84*

Abstract

The present paper seeks to publicize the importance and functionality of the BB84 protocol together with the Vernam's Encryption in the area of Quantum Cryptography. First, we will see the theoretical framework where we will address issues of Quantum Physics as the Principle of Superposition, Quantum entanglement, as well as what are bits and qubits, among others. These concepts will help us better understand the phases of quantum encryption. Finally, as an example, we will simulate the BB84 protocol and Vernam's Encryption, which will help us to encrypt a message.

Keywords: *Quantum Physics, Quantum Cryptography, Quantum Entanglement, Superposition Principle, Bits, Qubits, Vernam's Encryption, BB84 Protocol*

1. INTRODUCCIÓN

A lo largo de la historia, la humanidad ha tenido, por diversas razones, la necesidad de transmitir mensajes cuyo contenido deba permanecer oculto. Por ejemplo, es muy habitual ver noticias sobre ciberataques que ponen en jaque la seguridad de las compañías. Estas intrusiones tienen generalmente como finalidad acceder a datos relevantes, tales como claves de cuentas bancarias, tarjetas, informes médicos, conversaciones confidenciales, etc. Es por ello, que la criptografía nació, en principio, como la habilidad para esconder información a cualquier persona que no le estuviera permitido leerla. De ahí que, a través de los siglos, se desarrollaron distintas técnicas, métodos e instrumentos que permitieron el desarrollo de este arte.

En 1948, Claude Shannon propuso la Teoría de la Información, la cual establece que la información es mensurable. En consecuencia, la criptografía dio un salto importante: dejó de ser un arte para convertirse en una ciencia considerada como una rama de las matemáticas, ahora llamada Criptografía Moderna. Este hecho dio pie al surgimiento de diversos algoritmos criptográficos que se valen del uso de la computadora para su implementación. Por ejemplo, algunos métodos de cifrado de este tipo son: DES, el cual apareció en 1976 y fue aceptado como un estándar por el gobierno de Estados Unidos en 1977, y otros como el RSA (1977), el CCE (1985), el 3DES (1998) y, finalmente, el AES (2002).

Con la criptografía moderna se han desarrollado diversos algoritmos de cifrado basados en las matemáticas. Estos son

implementados en las computadoras y, mientras más complejo sea el algoritmo, más tardado y complejo será poder realizar un criptoanálisis (estudio del descifrado no autorizado de mensajes cifrados) sobre el mismo.

Uno de los algoritmos más utilizados en la actualidad es el RSA, el cual es un algoritmo de cifrado asimétrico, es decir, que trabaja con dos claves, una pública y una privada. Todo el contenido sin cifrar que sea hecho con la clave pública, podrá ser descifrado mediante la clave privada, y viceversa, todo contenido cifrado con la clave privada podrá ser descifrado mediante la clave pública. Esta es la base de algoritmos que usan el cifrado asimétrico.

Sin embargo, a pesar de que estos métodos de encriptación permiten en la actualidad mantener una comunicación segura entre dos partes, las propuestas algorítmicas de Shor en 1994, que nos permiten factorizar números primos en un tiempo polinomial, pondrían en peligro algunos sistemas criptográficos más usados, como el RSA. La criptografía cuántica puede lograr comunicaciones más seguras utilizando leyes de la naturaleza a escala cuántica, tales como el principio de incertidumbre de Heisenberg, la superposición cuántica y el enredo cuántico.

La criptografía cuántica utiliza la física para desarrollar un criptosistema completamente seguro para la tecnología actual y a largo plazo, puesto que no contamos aún con la existencia del computador cuántico. Este sistema criptográfico es distinto de las demás porque depende más de la física que de las matemáticas, como un aspecto clave de su modelo de seguridad. Actualmente en la criptografía cuántica existen algunos protocolos criptográficos como el Protocolo E91, el Protocolo B92 y el Protocolo BB84 que detallaremos más adelante.

El objetivo del presente proyecto es documentar los conceptos básicos de la criptografía cuántica, algunos avances sobre el tema, así como describir generalidades de la mecánica cuántica e ilustrar algunos conceptos de ésta que son relevantes para el estudio de la encriptación cuántica. Análogamente, se pretende abarcar de la manera más simplificada y directa posible los fundamentos de la criptografía cuántica, que es la única aplicación comercial existente hasta la fecha de la Teoría de la Información Cuántica, sirviendo como una introducción al tema, y una motivación para futuros estudios.

2. CONCEPTOS PREVIOS

Antes de empezar a estudiar la criptografía cuántica y los protocolos QKD, tenemos que repasar algunos conceptos relacionados con la criptografía y la mecánica cuántica.

2.1. Entrelazamiento cuántico:

Dos partículas cuánticas pueden tener estados fuertemente correlacionados, debido a que se generaron al mismo tiempo o a que interactuaron. Cuando esto ocurre se dice que sus estados están entrelazados, lo que provoca que la medición sobre una de ellas determina inmediatamente el estado de la otra, sin importar la distancia que las separe.

Este comportamiento "mágico" es de gran interés para la criptografía cuántica, puesto que nos permitirán implementar un sistema muy especial para la distribución de claves.

2.2. Principio de Incertidumbre:

El principio nos asegura que es imposible determinar, con precisión absoluta y de forma simultánea, el valor de dos magnitudes conjugadas de un sistema elemental. Ejemplos de estos son posición y momento, energía y tiempo, o tiempo y frecuencia.

Si se mide una propiedad, necesariamente se altera la complementaria, perdiéndose cualquier noción de su valor exacto. Cuanto más precisa sea la medición sobre una propiedad, mayor será la incertidumbre de la otra propiedad.

2.3. Principio de Superposición:

El principio de superposición viene a afirmar que un sistema cuántico puede poseer simultáneamente dos o más valores de una cantidad observable, valores que pueden ser incluso contradictorios. Algo que se sale completamente de lo que podemos entender por razonable, pero que es clave para conocer el comportamiento de los sistemas que queremos implementar.

2.4. Teorema de la no clonación:

Este teorema nos asegura que "no pueden existir máquinas o dispositivos de clonación cuánticas".En otras palabras, no es posible hacer copias exactas de la información cuántica, debido a que en el intento de obtener información acerca de este, la misma medición provoca su modificación.

El teorema significó un gran avance para el desarrollo de la teoría de la información cuántica como la criptografía cuántica. Si fuera posible para un espía copiar los estados cuánticos mientras viajan del emisor al receptor, la criptografía cuántica no tendría sentido.

2.5. Computación Cuántica:

Con la llegada de la teoría cuántica y algunas de sus propiedades, como superposición y entrelazamiento cuántico (que ya se conceptualizaron anteriormente), se predijo que los computadores cuánticos, definidos como "un tipo de computador que explota las interacciones de la mecánica cuántica",podrían desarrollar ciertas tareas computacionales exponencialmente más rápido que cualquier ordenador clásico. Dichas predicciones van de la mano con los desarrollos de algoritmos cuánticos, que desde una base teórica, aprovechan las características de la teoría cuántica.

La computación cuántica se basa en el uso de qubits, una combinación de unos y ceros, en lugar de bits, en los que solo se usa el 1 o el 0, no pueden estar a la vez. Esto da lugar a nuevas puertas lógicas que hacen posibles nuevos algoritmos.

Las ventajas que aporta la computación cuántica son la aplicación masiva de aplicaciones en paralelo y la capacidad de aportar nuevas soluciones a problemas que no son abarcables por la computación cuántica debido a su elevado coste computacional.

2.6. Polarización de un fotón:

Los fotones parecen ser el mejor medio para transportar información cuántica en grandes distancias. Son partículas sin masa, que se mueven a la velocidad de la luz, y que no tienen carga eléctrica. Además se producen y se detectan fácilmente, y la transmisión por fibra óptica de los fotones con una longitud de onda específica es lo suficientemente confiable como para aplicaciones prácticas. Una de las propiedades de los fotones de las que se vale la criptografía cuántica para codificar un bit es la polarización, que se refiere al plano en el que oscila el campo eléctrico mientras el fotón se propaga.

	Polarización rectilínea	Polarización diagonal
Estado $\|0\rangle$ Fotón polarizado en 0° o 45°	↔	↗
Estado $\|1\rangle$ Fotón polarizado en 90° o 135°	↕	↘

Figura 1: Estados de polarización

2.7. Qubit:

En los ordenadores clásicos la mínima cantidad de información almacenable es el bit. Una celda de memoria atómica puede almacenar uno de dos posibles estados discretos, el 0 o el 1. La aplicación de la mecánica cuántica al concepto de bit es lo que permite el nacimiento del bit cuántico o qubit (quantum bit): una celda de memoria que puede encontrarse en uno de los dos estados (0 ó 1), o en una determinada superposición de ambos.

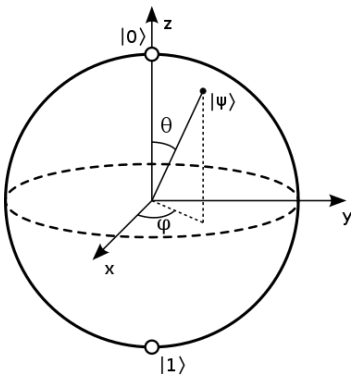

Figura 2: Representación gráfica de un qubit en forma de esfera de Bloch

2.8. Criptografía:

La criptografía es el estudio de técnicas matemáticas y en la actualidad también informáticas relacionadas con aspectos de la seguridad de la información tales como la confidencialidad, integridad de datos, autenticación de entidades, y autenticación de origen de los datos. La criptografía no es el único medio de proveer seguridad de la información, sino un conjunto de técnicas.

Es importante mencionar que los esquemas de cifrado no son invulnerables. Por ejemplo, un espía, después de invertir un periodo de tiempo atacando el código, podría descifrar los datos. Este periodo de tiempo es importante porque la vida

útil de la clave debe estar correlacionada con la vida útil de los datos que están siendo protegidos.En algunos casos un día es suficiente, mientras que en otros debería permanecer invulnerable de manera indefinida.

2.9. Crifrado de Vernam:

El cifrado Vernam es un algoritmo de criptografía inventado por Gilbert Vernam en 1917. EL método consiste de un alfabeto binario de ceros y unos, su funcionamiento es bastante simple consistiendo en un único cálculo de una operación XOR (ó exclusivo) entre cada segmento del mensaje a cifrar y una clave previamente compartida. Esta única operación sirve tanto para el cifrado, como para el descifrado del mensaje, y debe aplicarse sobre segmentos de tamaño similar a la clave utilizada. Si la clave es escogía aleatoriamente y no se usa nuevamente el cifrado, es llamado one-time pad(libreta de un solo uso). Este cifrado es el que usaremos para encriptar nuestro mensaje más adelante.

2.10. Criptografía Cuántica:

La criptografía cuántica es una de las áreas más recientes en investigación dentro de la criptografía, está basada en los principios de la mecánica cuántica para transmitir y proteger la información, de manera que solo pueda ser accedida por los usuarios autorizados. Su desarrollo surge de la investigación de la computación cuántica como un medio a futuro para proteger la información de manera que esta continúe siendo segura y su transmisión sea más confiable y privada.

El estudio y desarrollo de la criptografía cuántica está enfocada a la investigación de un Protocolo de Distribución de Clave Cuántica (QKD).

La característica que distingue QKD del cifrado estándar es que las claves se transmiten como fotones, generalmente partículas de luz, de tal manera que si un tercero intercepta una, la ley física de la observación entra en juego: observar algo es cambiarlo.

Pueden existir varias partículas simultáneamente en más de un lugar y un estado. Basta con elegir cómo deben comportarse cuando entran en contacto con algo diferente o cuándo se miden, así la clave también cambia al instante, pasa a ser ilegible y, por consiguiente, inútil. Esta modificación también indica al destinatario previsto que su contenido ha resultado comprometido.

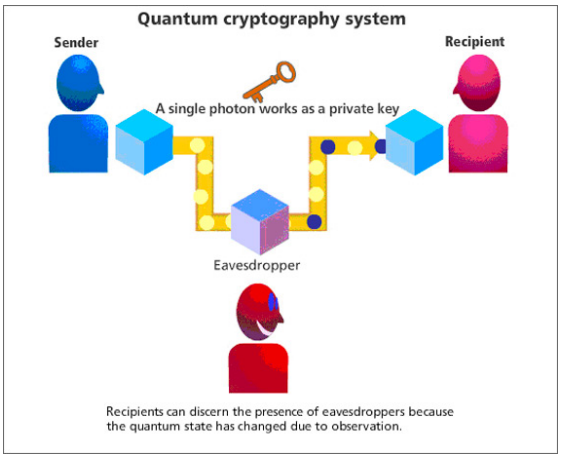

Figura 3: Representación de un sistema de encriptación cuántico

Como ya hemos mencionado en la introducción, la criptografía cuántica utiliza varios protocolos, en este artículo profundizaremos en el protocolo BB84, puesto que es el más utilizado en la actualidad.

3. ANÁLISIS

3.1. Protocolo BB84:

Uno de los primeros avances de la criptografía cuántica,*el protocolo BB84*,de la serie de protocolos llamados QKD, (Quantum Key Distribution), **propuesto por Charles Bennett y Gilles Brassard en 1984** (de ahí que se le conoce como BB84) en la International Conference on Computers, Systems and Signal.

El protocolo BB84 **está basado en la transmisión individual de qubits ("quantum bit")** que formarán la clave final del mensaje enviado donde **se usará dos canales de comunicación, el canal público (bidireccional) y el canal cuántico (unidireccional)** que en general es de fibra óptica, material que no conduce electricidad, por el que se envían pulsos de luz que presentan datos a transmitir (Figura 4).

En un caso ideal el canal cuántico está libre de ruido en la transmisión. Cuando un espía intenta interceptar la transmisión de fotones, intentará enviar una copia de los fotones originales interceptados que se generó por el emisor, pero por el teorema de no clonación, que básicamente declara que es imposible crear una copia idéntica de un estado cuántico desconocido arbitrario, esto no es posible.

Los protagonistas serán Alice y Bob, donde Alice quiere enviar un mensaje a Bob, pero no sabe cómo hacerlo para tener la seguridad de que Eva no va a leerlo por el camino, así que recurre a la mecánica cuántica, donde interactúan un conjunto de qubits implementados en fotones con cuatro estados de polarización(Figura 5).

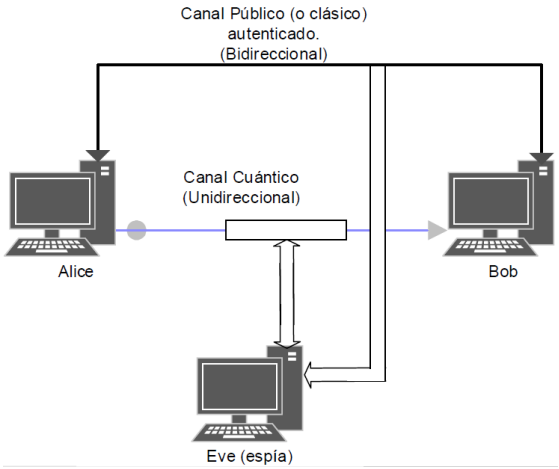

Figura 4: Representación del protocolo BB84.

Alice y Bob se comunican por teléfono (canal público), donde establecerán un convenio de signos para la clave. En primer lugar, eligen dos bases y cada base con componentes ortonormales (vectores ortogonales y con norma igual a 1) (Figura 5).

Base	Polarización	Valor del *qubit*
B_+	↔	Polarización del fotón en horizontal con el valor lógico binario 0.
B_+	↕	Polarización del fotón en vertical con el valor lógico binario 1.
$B_\times$	⤢	Polarización del fotón en diagonal a la izquierda con el valor lógico binario 0.
$B_\times$	⤡	Polarización del fotón en diagonal a la derecha con el valor lógico binario 1.

Figura 5: Nomenclatura de los estados de polarizacion en función de la base y el valor asociado.

Tener en cuenta que un estado de polarización es correcto al pasar por un polarizador correspondiente a su base (+ o X), de otra manera la polarización se orienta de manera aleatoria si pasa por un polarizador que tenga otra base.

Ahora Alice es el transmisor y tiene una máquina que elige al azar, tanto la base que va a usar como el bit que va a enviar, teniendo una secuencia de fotones polarizados (Figura 6).

(+)	(X)	(X)	(+)	(+)	(X)	(+)	(X)	(X)	(X)	(+)	(X)	(+)	(+)	(+)	(X)
1	0	1	1	0	0	1	1	1	0	1	0	0	0	1	0
|	/	\	|	–	/	|	\	\	/	|	/	–	–	|	/

Figura 6: Secuencia de fotones polarizados enviados por Alice.

Y a continuación usa el canal cuántico para enviar a Bob los fotones polarizados,donde Bob recibe la secuencia completa de fotones polarizados generados por Alice, y usará un aparato basado en polarizadores para medir la polarización de los fotones, pero sin saber Bob, que bases ha usado Alice, así que Bob tendrá que elegir al azar las bases para cada fotón. Esto provocará que la mitad de las veces elija una base que no se corresponda, veamos lo que mide Bob (Figura 7).

(+)	(+)	(X)	(+)	(X)	(+)	(+)	(+)	(X)	(X)	(X)	(+)	(X)	(X)	(+)	(X)
|	–	\	|	\	–	|	–	\	/	/	\	/	/	|	/
1	0	1	1	1	0	1	0	1	0	0	1	0	0	1	0

Figura 7: Secuencia de medición hecho por Bob, de los fotones polarizados enviados por Alice.

Una vez que Bob ha recibido la secuencia completa de qubits generados por Alice, ambos interlocutores vuelven a ponerse en contacto. En esta llamada, lo que hace Alice es decirle a Bob qué bases ha usado, y Bob le dice en cuáles ha acertado (Figura 8).

(+)	(X)	(X)	(+)	(+)	(X)	(+)	(X)	(X)	(X)	(+)	(X)	(+)	(+)	(+)	(X)
1	0	1	1	0	0	1	1	1	0	1	0	0	0	1	0
|	/	\	|	–	/	|	\	\	/	|	/	–	–	|	/
(+)	(+)	(X)	(+)	(X)	(+)	(+)	(+)	(X)	(X)	(X)	(+)	(X)	(X)	(+)	(X)
|	–	\	|	\	–	|	–	\	/	/	\	/	/	|	/
1	0	1	1	1	0	1	0	1	0	0	1	0	0	1	0

Figura 8: Cuadro de comparación de las bases dadas por Alice y las bases con los que midió Bob los fotones polarizados.

Después de quedarse con las bases que coinciden (Figura 9), se tiene 8 bits que coinciden tanto para Alice como para Bob.

(+)	(X)	(+)	(+)	(X)	(X)	(+)	(X)
1	1	1	1	1	0	1	0

Figura 9: El cuadro representa los bits en donde las bases de Alice y Bob coinciden.

Ahora qué pasaría si Eva estuviera escuchando en medio. Para ello Eva lo que va a hacer es por un lado escuchar por el teléfono, para enterarse de todo lo que hablan e interceptar todos los fotones y reenviarlos a Bob (Figura 10).

Base de Alice	(+)	(X)	(X)	(+)	(+)	(X)	(+)	(X)	(X)	(X)	(+)	(X)	(+)	(+)	(+)	(X)
Bit de Alice	1	0	1	1	0	0	1	1	1	0	1	0	0	0	1	0
Polarización de Alice	|	/	\	|	–	/	|	\	\	/	|	/	–	–	|	/
Base de Eva	(+)	(+)	(+)	(+)	(X)	(X)	(+)	(X)	(+)	(+)	(X)	(X)	(+)	(X)	(X)	(X)
Polarización de Eva	|	–	–	|	\	/	|	\	–	|	/	/	–	\	\	/
Bit de Eva	1	0	0	1	1	0	1	1	0	1	0	0	0	1	1	0
Base de Bob	(+)	(X)	(X)	(+)	(+)	(X)	(+)	(X)	(X)	(X)	(+)	(+)	(X)	(+)	(X)	(+)
Polarización de Bob	|	\	/	|	–	/	|	\	/	\	–	|	/	–	\	–
Bit de Bob	1	1	0	1	0	0	1	1	0	1	0	1	0	0	1	0

Figura 10: Secuencia de fotones polarizados dado Alice, Eva y Bob

Y una vez que se completó el proceso de enviar y recibir fotones, esta vez con Eva espiando, pasan a la parte de la llamada telefónica para ver qué bases están equivocadas y ahora Eva solo se puede dedicar a escuchar y ver qué pasa.

Base de Alice	(+)	(X)	(X)	(+)	(+)	(X)	(+)	(X)	(X)	(X)	(+)	(+)
Bit de Alice	1	0	1	1	0	0	1	1	1	0	1	0
Polarización de Alice	/	\	|	–	/	|	\	\	/	|	–	
Base de Eva	(+)	(+)	(+)	(+)	(X)	(X)	(+)	(X)	(+)	(+)	(X)	(X)
Polarización de Eva	|	–	–	|	\	/	|	\	–	|	/	\
Bit de Eva	1	0	0	1	1	0	1	1	0	1	0	1
Base de Bob	(+)	(X)	(X)	(+)	(+)	(X)	(+)	(X)	(X)	(X)	(+)	(+)
Polarización de Bob	|	\	/	|	–	/	|	\	/	\	–	–
Bit de Bob	1	1	0	1	0	0	1	1	0	1	0	0

Figura 11: El cuadro representa las bases que coinciden dadas por Alice y Bob,y los fotones polarizados medidos por Eva, en cuya posición donde Alice y Bob coincidieron.

Ahora, Alice y Bob sabiendo que usaron las mismas bases, sus claves deben ser iguales, por lo que para asegurarse, toman un fragmento de prueba y las comparan en una canal abierto (Figura 12).

Clave de Alice	1	0	1	1	0	0	1	1	1	0	1	0
Clave de Bob	1	1	0	1	0	0	1	1	0	1	0	0

Figura 12: Cuadro de comparación de los bits de Alice y Bob en las bases que coincidieron.

En el proceso de comparación de las bases, sucede que Alice y Bob coinciden con las bases, pero no coinciden con los estados medidos, y se dan cuenta de que hay muchos errores cuando no debería haberlos y eso solo significa que alguien ha estado escuchando, ¡ajá! El espía queda al descubierto y por tanto es mejor no enviar nada hasta que quien sea deje de espiar.

Conclusión: Este protocolo es propuesto para el intercambio seguro de claves entre Alice y Bob. Alice y Bob intentan acordar una clave utilizando el cifrado cuántico, donde la clave resultante o final es utilizada para cifrar información.

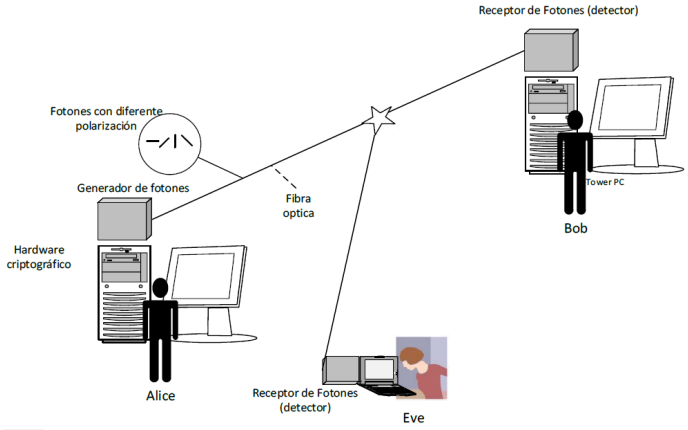

Figura 13: Protocolo BB84 de la criptografía cuántica.

3.2. Cifrado de Vernam:

Alice y Bob al finalizar el protocolo BB84, ya se habrá definido una clave, que será utilizada para encriptar y desencriptar el mensaje con el cifrado de Vernam(Figura 14)

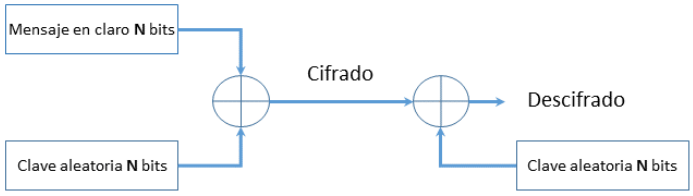

Figura 14: Representación del Cifrado de Vernam

El cifrado de Vernam requiere una clave aleatoria en minúsculas de la misma longitud que el mensaje a enviar, que debe estar en mayúsculas y sin espacios, realizando un XOR (Figura 24) ,cuyo símbolo es $\oplus$, entre el código binario ASCII de cada carácter del mensaje y de la clave, obteniendo así el mensaje cifrado.

A	B	A XOR B
0	0	0
0	1	1
1	0	1
1	1	0

Figura 15: Compuerta lógica XOR

Para descifrar el mensaje se requiere el mensaje encriptado y la clave, donde el algoritmo que revierte el cifrado, será realizar un XOR entre el mensaje encriptado y la clave. Para que quede claro el cifrado de Vernam encriptaremos el mensaje "H" con la clave "p".

Paso 1: Cifraremos el mensaje "H" con la clave "p"(Figura16, Figura 17).

Mensaje	H
Código	0100 1000
Clave	p
Código	0111 0000

Figura 16: Mensaje y clave aleatoria con sus respectivos códigos.

H	P	H $\oplus$ p
0	0	0
1	1	0
0	1	1
0	1	1
1	0	1
0	0	0
0	0	0
0	0	0

Figura 17: Codigo binario del Mensaje Encriptado.

Y asi obteniendo el mensaje cifrado(Figura 18)

Mensaje Cifrado	**8**
Código	0011 1000

Figura 18: Mensaje Encriptado.

Paso 2: Ahora para descifrar el mensaje encriptado realizamos un XOR con el mensaje encriptado "8" y la clave "p"(Figura19).

8	p	8 $\oplus$ p
0	0	0
0	1	1
1	1	0
1	1	0
1	0	1
0	0	0
0	0	0
0	0	0

Figura 19: Código binario del Mensaje Desencriptado.

Ahora ya obtenido el código binario, buscamos en la tabla ASCII para obtener el mensaje desencriptado(Figura 20).

	8 $\oplus$ p
Código	0100 1000
Mensaje	H

Figura 20: Mensaje Desencriptado.

Y se observa que se obtiene el mensaje que se quería enviar, así finalizando con el cifrado de Vernam.

Unos puntos a tener en cuenta:

- Si la longitud de la clave es menor a la longitud del mensaje, se tendrá que repetir la clave hasta tener la misma longitud que el mensaje.
  Ejemplo:
  Mensaje : MATEMATICA (longitud 10)
  PseudoClave : abcd (longitud 4)
  Clave final : abcdabcdab (longitud 10)

- Si la longitud de la clave es mayor a la longitud del mensaje, se tendrá que recortar la clave.
  Ejemplo:
  Mensaje : nota (longitud 4)
  Pseusdoclave : parcialesfinales (longitud 16)
  Clave final : parc (longitud 4)

4. MODELAMIENTO

PROTOCOLO BB84 SIN ESPIAS

Fase 1:

Para empezar, el programa nos pide ingresar la tasa de espionaje, digitamos 0 para ver una simulación sin espías, y un número en un rango de]0,1] para indicar la probabilidad de espionaje.

Luego digitamos el número de qubits que deseamos que se envíen Alice y Bob, si queremos que solo se genere 1 qubit

entonces presionamos el botón de "Simular un qubit", y si deseamos más de 1 qubit entonces digitamos la cantidad que queramos que se genere. Teniendo como función principal a **create_qubit** (Figura 21).

```
def create_qubit(self, bit_=None, basis_=None):
    if bit_==None or basis_==None:
        #crea un bit y una base aleatorios
        if random.random()<0.5:
            bit = 0
        else:
            bit = 1
        self.bit_array.append(bit)
        basis = self.choose_basis()
        self.basis_array.append(basis)
    else:
        #guarda el bit y la base ingresados
        bit = bit_
        basis = basis_
    #retorna un qubit en una matriz
    return self.get_density_matrix(bit, basis)
```

Figura 21: Función que genera qubits aleatoriamente

Ulteriormente, se muestran los bits, las bases de los qubits y los fotones polarizados, expresados con flechas, que Alice envía a Bob, asimismo, los bits que corresponden a las bases elegidas por Bob aleatoriamente.

En el caso de que Eva esté presente, además se simulará los fotones que ella interceptó, las bases que eligió y su bit coerrespondiente. Cabe recalcar que si Eva intenta medir los fotones que mandó Alice, introduciría una perturbación en los fotones enviados por Alice si no coinciden en la base.

Fase 2:

Seguidamente comparamos las bases de los qubits de Alice y Bob usando la función **compareBasis** (Figura 22).

```
def compareBasis(self, number):
    if self.a.basis_array[number]==self.b.basis_array[number]:
        for person in self.peopleList:
            if person.name!="Eve" or self.compareBasisE(number):
                person.keepBit(number)
            else:
                person.keepBit(-1)
        return True
    else:
        return False
```

Figura 22: Función que compara las bases entre dos qubits

Luego aparecerán resaltados en verde las bases en las que ambos (Alice y Bob) coincidieron y las bases en las que no coinciden serán descartados. Los bits seleccionados serán mostrados en la parte inferior de la ventana.

Fase 3:

Alice y Bob elijirán una cantidad de bits, en este caso 6 bits, para compararlos por el canal público. Estos bits se muestran resaltados con color naranja, y así el programa halla la tasa de error mediante la función **error_rate**(Figura 23), resultando en este caso 0.0.

```
def error_rate(self):
    number = int(self.getNumber("int"))
    while number==None:
        number = self.getNumber("int")
    if number > self.channel.a.getArrayLength():
        number == self.channel.a.getArrayLength()-1
    #subconjunto de bits diferentes
    subset = self.channel.getSubset(number)
    counter = 0
    for i in subset:
        #cardinal del subconjunto
        if self.channel.compareBit(i)==False:
            counter+=1
    #cálculo del error
    error=float(counter)/float(len(subset))
    return error
```

Figura 23: Función que calcula la tasa de error

Luego aparece el mensaje "¿Quieres abortar o continuar con el proceso?",en el caso sin espías elegiremos continuar ya que la tasa de error es menor a 0.03. Por otro lado, en el caso de haber espías se tiene que abortar ya que la tasa de error es mayor a 0.03.

Fase 4:

Finalmente Alice y Bob obtienen una clave formada por los qubits que no han sido comparados.

CIFRADO DE VERNAM

Fase 5:

Luego, pasamos a la siguiente fase, el Cifrado de Vernam. El algoritmo consiste en convertir el mensaje a binario, seguidamente el programa realiza la operación XOR (Figura 24) con la cual se encriptará nuestro mensaje. Por último desencriptamos el mensaje para así poder comprobar que el mensaje ha sido encriptado y desencriptado con éxito.

```
def XOR(self, msg, key):
    cryp = ''
    for i in range(len(msg)):
        if msg[i] == key[i]:
            cryp += '0'
        else:
            cryp += '1'
    return cryp
```

Figura 24: Función que realiza la operación XOR entre dos string

5. IMPACTO Y APLICACIONES

En definitiva, es un hecho que la ciberseguridad cambiará radicalmente en los próximos años, pues con la llegada de la computación y la criptografía cuántica **se pondrá**

en riesgo toda la criptografía asimétrica utilizada actualmente en internet, telefonía, por gobiernos o por agencias de inteligencia.

El Instituto Europeo de Estándares en Telecomunicaciones (ETSI), en un documento mucho más amplio publicado en 2015, considera a la criptografía cuántica como la única alternativa segura de encriptación a largo plazo y analiza su funcionamiento, ventajas y desafíos. **Asimismo, describe casos de uso de distribución de claves cuánticas (QKD) como encriptación y autenticación, infraestructura de redes, almacenamiento en la nube o inteligencia artificial, y campos de aplicación como medicina y salud, servicios financieros o aplicaciones móviles.**

5.1. Impacto social por sectores:

El desarrollo de esta nueva tecnología, cambiará la vida de las personas tanto directa como indirectamente pues **sectores y ramas como medicina, biología y genética, economía y finanzas, política y seguridad militar y, principalmente, en informática dispondrán de una nueva generación de seguridad tecnológica cuántica.**

Figura 25: Impacto y aplicaciones de la Criptografía cuántica por sectores

5.2. Impacto comercial internacional:

Muchas de las compañías trabajando en el desarrollo de redes 5G ya se están enfocando en hacerlas quantum-safe, es decir, resistente a la computación cuántica y su capacidad de hackeo de las telecomunicaciones actuales.

Entre ellas, se destaca el trabajo de la **compañía surcoreana SK Telecom**, que en 2017, firmó un acuerdo con la **compañía alemana Deustche Telekom** para *"garantizar telecomunicaciones seguras en la era cuántica"* y otro acuerdo con **Nokia** para *"trabajar conjuntamente en criptografía cuántica"*. Además, en 2018, invirtió en la compañía suiza IDQuantique, líder en manufacturación de tecnología cuántica para criptografía. Estas alianzas han dado ya sus frutos, como por ejemplo *la realización de pruebas con generadores cuánticos de números aleatorios y protocolos de criptografía simétrica cuántica*, también se reportó *la realización de pruebas satisfactorias de interoperabilidad entre los sistemas de criptografía asimétrica de IDQuantique y la solución de Transporte Óptico Seguro de Nokia.*

En Corea del Sur, además, **SK Telecom**, **KT** y **LG Uplus** están asesorando a la **Unión Internacional de Telecomunicaciones (ITU)** que establezcan estándares para poder **construir redes de telecomunicaciones que incorporen 5G y criptografía cuántica que sean interoperables a nivel mundial**.

Cambiando de continente, la nueva **compañía estadounidense Quantum Xchange** está desarrollando *la primera red comercial con criptografía cuántica de Estados Unidos que "conectará los mercados financieros de Wall Street con centros de respaldo en Nueva Jersey, permitiendo mantener información confidencial segura"*.

6. RESULTADOS

El presente trabajo desarrolló una implementación por medio de código para simular el Protocolo BB84 y el Cifrado de Vernam, utilizando para este fin el lenguaje de programación Python. Para el primer código diseñamos una interfaz gráfica que nos permitió mostrar los bits y fotones polarizados así como la tasa de error al comparar los resultados de ambos personajes, el cual tuvo resultados muy favorables. Por otro lado, al programar el algoritmo de Vernam también se obtuvo los resultados esperados, sin embargo por fines prácticos es mejor visualizarlos por separado para entender cómo funciona cada parte del proceso.

7. CONCLUSIONES

Es cuestión de tiempo para que los primeros computadores cuánticos, que permitan ejecutar algoritmos como el de Shor, representen una amenaza para los esquemas criptográficos más usados hoy en día por todos. Como solución a este y otros problemas, se justifica la aplicación de la crip-

tografía cuántica, y es por ello que ya existen empresas dedicadas a crear redes seguras usando la libreta de un solo uso y la criptografía cuántica.

La distribución de claves cuánticas es una poderosa herramienta dentro de la transmisión de información de manera segura entre usuarios remotos, que muy seguramente se volverá imponente en los próximos años, ya que le permite acordar una clave segura que será utilizada en la transmisión de un mensaje privado, por medio de un canal inseguro, siendo independiente de cualquier valor de entrada; algo imposible para la criptografía clásica.

La mecánica cuántica no proporciona un método de cifrado tal cuál, sino que complementa al cifrado de Vernam proporcionando un protocolo de distribución de clave seguro, en este caso se utlizó el protocolo BB84, siendo este el más usado para pruebas de encriptación cuántica.

El protocolo de cifrado de Vernam es el que se usa comúnmente en criptografía cuántica ,debido a ser de los cifrados más sencillos y el único que se ha demostrado que es irrompible.

Aunque la criptografía cuántica no sea muy práctica hoy en día, es la rama de la computación cuántica que más presenta avances y que tiene implicaciones más severas en sus resultados. A diferencia de los sistemas criptográficos asimétricos, su seguridad ha sido demostrada 100 % segura sin importar con qué recursos computacionales se cuente

8. SUGERENCIAS

Partiendo de los resultados y conclusiones en los apartados anteriores, por último sugerimos algunas ideas para iniciar futuras investigaciones y comprender con mayor exactitud que es la criptografía cuántica. .Leer críticamente las referencias de la bibliografía, donde se podrá ahondar sobre la criptografía cuántica. .Investigar sobre la computación Cuántica, ¿qué es, existirá, y en que afectaría a la criptografía cuántica? .Darnos cuenta el avance de la criptografía cuántica sobre la criptografía convencional.

9. BIBLIOGRAFÍA

1. L. Cáceres, R. Fritis, P. Collao. *Desarrollo de un simulador para el protocolo de criptografía cuántica E91 en un ambiente distribuido.* Ingeniare. (2014). Recuperado de https://scielo.conicyt.cl/pdf/ingeniare/v23n2/art09.pdf

2. J. Martínez. *Criptografía cuántica aplicada.* Universidad Politécnica de Madrid. (2008). Recuperado de http://oa.upm.es/1298/1/PFC_JESUS_MARTINEZ_MATEO.pdf

3. H. Ortiz. *Fundamentos de criptografía cuántica.* Universidad EAFIT. (2007). Recuperado de https://core.ac.uk/reader/47241786

4. Página web: https://www.gaussianos.com/criptografia-protocolo-de-distribucion-de-clave-bb84/

5. Página web: https://es.wikipedia.org/wiki/Criptograf %C3 %ADa_cu %C3 %A1ntica#: :text=La %20criptograf %C 3 %ADa %20cu %C3 %A1ntica %20es %20la,se %20publica % 20el %20primer %20protocolo.

6. V. Díaz. *Implementación del protocolo de distribución cuántica de claves, protocolo BB84.* Universidad Nacional Autónoma de México. (2015). Recuperado de http://132.248.9.195/ptd2015/mayo/0729819/0729819.pdf

7. Página web: https://es.wikipedia.org/wiki/Teorema_de_no _clonaci %C3 %B3nB3n

8. Pagina web: https://es.dynabook.com/generic/toshibytes-blogpost12-quantum-cryptography/

9. V. Aranibar, A. Rioja. *Implementación de una aplicación de cifrado y descifrado de mensajes mediante Verman, utilizando el lenguaje de programación Flash.* (2017). Recuperado de https://aranibarvictor.wordpress.com/2017/05/18/implementacion-de-una-aplicacion-de-cifrado-y-descifrado-de-mensajes-mediante-verman-utilizando-el-lenguaje-de-programacion-flash/

10. Página web: http://numerentur.org/cifrado-vernam/

11. M. López. *Tecnologías Cuánticas: Una oportunidad transversal e interdisciplinar para la transformación digital y el impacto social.* Banco Interamericano de Desarrollo. (2019). Recuperado de https://publications.iadb.org/publications/spanish/document/Tecnolog %C3 %ADas_cu %C3 %A1nticas_Una_oportunidad_transversal_e_interdisciplinar_para_la_transformaci %C 3 %B3n_digital_y_el_impacto_social.pdf

ANEXO

Interfaz Gráfica

Simulación de la emisión y recepción de un mensaje mediante criptografía cuántica