

METODOLOGÍA DE LA INVESTIGACIÓN

ACTIVIDAD 2

Tutor: Rosa González

Estudiante: José Ramón Ibáñez Posadas

Matricula: BNL098377

INTRODUCCIÓN

La encriptación y la seguridad de la información son temas de vital importancia en la era digital, donde proteger la confidencialidad y la integridad de los datos se ha vuelto imperativo. Sin embargo, con el avance de la computación cuántica, la seguridad de los sistemas de encriptación tradicionales se ha visto amenazada.

En esta introducción, se explorará la intersección entre la encriptación tradicional y la computación cuántica. La encriptación tradicional se basa en algoritmos y protocolos que han sido ampliamente utilizados y considerados seguros en entornos de computación clásica. Sin embargo, los avances en la computación cuántica plantean la posibilidad de que estos algoritmos sean vulnerables a ataques cuánticos más eficientes.

La computación cuántica, basada en principios de la mecánica cuántica, promete una capacidad de cálculo exponencialmente superior a la de las computadoras clásicas. Esto plantea interrogantes sobre cómo mantener la seguridad de la información en un mundo donde las computadoras cuánticas podrían romper fácilmente los sistemas criptográficos tradicionales.

En consecuencia, el campo de la encriptación cuántica ha surgido como una solución potencial para este problema. La encriptación cuántica se basa en los principios de la mecánica cuántica para garantizar una seguridad intrínseca a nivel de partículas subatómicas, lo que la hace potencialmente resistente a los ataques cuánticos. Sin embargo, su implementación práctica y los desafíos asociados plantean preguntas acerca de la viabilidad y la compatibilidad con los sistemas existentes.

En esta investigación, se examinará el marco teórico, los avances más recientes en la investigación de la criptografía cuántica y los desafíos de implementación práctica de la encriptación cuántica. También se destacarán las contribuciones de importantes autores y académicos en este campo de estudio. A través de este análisis, se busca comprender mejor los retos y las oportunidades que presenta la combinación de la encriptación tradicional y la computación cuántica, y cómo podemos garantizar la seguridad de la información en un entorno de constante evolución tecnológica.

Carrera:

Ingeniería en Tecnologías Computacionales

***Tetramestre:**

1

***Tema de investigación**

Este debe ser enfocado a tu carrera.

La Encriptación tradicional contra la Computación Cuántica

***Descubrimiento del problema**

Debe ser una situación a resolver presente sobre el objeto de investigación.

se busca desarrollar métodos de encriptación que sean seguros contra los ataques cuánticos y puedan proteger la información en un entorno de computación cuántica. Esta área de investigación es crucial para garantizar la seguridad de la información en el futuro, a medida que la tecnología cuántica continúa avanzando.

***Preguntas de investigación**

Citar al menos 3 preguntas que te ayuden a resolver el problema.

- 1. ¿Cuáles son los algoritmos de encriptación tradicional más comunes y cuáles de ellos podrían ser vulnerables a ataques cuánticos?*
- 2. Cuáles son los avances más recientes en la investigación de la criptografía cuántica?*
- 3. ¿Cuáles son las implicaciones y desafíos de implementar la encriptación cuántica en entornos prácticos?*

***Objetivos**

(Debe mostrar las metas a alcanzar en el proyecto de investigación) (Un objetivo general y al menos dos objetivos específicos)

Objetivo General: es desarrollar métodos de encriptación cuántica que sean seguros y resistentes a los ataques cuánticos, garantizando la protección efectiva de la información en un entorno de computación cuántica.

Objetivos Específicos:

- 1. Investigar y desarrollar algoritmos y protocolos de encriptación cuántica*
- 2. Evaluar la viabilidad y los desafíos de la implementación práctica de la encriptación cuántica*

***Teoría de la investigación**

El marco teórico debe considerar:

*Estar fundamentado en al menos 2 fuentes de consulta viables (no blogs, no wikis).
Citar autores dentro del documento en formato APA.*

La encriptación tradicional se refiere a los métodos clásicos de cifrado utilizados en la información digital, que se basan en la teoría de la información y la criptografía clásica. Estos métodos se han utilizado durante décadas y se consideran seguros en entornos de computadoras clásicas. Sin embargo, la computación cuántica es una tecnología emergente que utiliza qubits, unidades de información cuántica, para realizar cálculos y procesar información de manera más eficiente que las computadoras clásicas. Se ha planteado la preocupación de que los algoritmos de encriptación utilizados actualmente podrían ser vulnerables a los ataques cuánticos, ya que los computadores cuánticos podrían ser capaces de factorizar grandes números primos de manera más rápida y eficiente.

Shor, P. W. (1994). Algorithms for quantum computation: Discrete logarithms and factoring. En Proceedings of the Annual Symposium on Foundations of Computer Science (FOCS) (pp. 124-134). IEEE.

Peter Shor es un destacado científico de la computación cuántica que presentó el famoso algoritmo de Shor en 1994. Este algoritmo fue un hito importante y demostró cómo la computación cuántica podría factorizar grandes números primos de manera mucho más eficiente que los algoritmos clásicos. Su trabajo puso de relieve la amenaza que los computadores cuánticos podrían representar para la encriptación tradicional.

Gisin, N., Ribordy, G., Tittel, W., & Zbinden, H. (2002). Quantum cryptography. *Reviews of Modern Physics*, 74(1), 145-195.

Nicolas Gisin y sus colaboradores son reconocidos por sus contribuciones al campo de la criptografía cuántica. Su artículo en la revista *Reviews of Modern Physics* proporciona un panorama completo de los principios y protocolos de la criptografía cuántica, incluyendo la teoría detrás de la distribución cuántica de claves y el intercambio seguro de información utilizando principios de la mecánica cuántica.

Descripción de muestras e instrumentos

1. ¿Hace cuanto tomaste algún curso/taller/diplomado referente a seguridad informática?

- ☐ Nunca
- ☐ 1 o 2 años
- ☐ 3 o 4 años
- ☐ + 5 años

2. ¿Hace cuanto tomaste algún curso/taller/diplomado referente a computación cuántica?

- ☐ Nunca
- ☐ 1 o 2 años
- ☐ 3 o 4 años
- ☐ + 5 años

3. ¿Crees que la computación cuántica llegue a desplazar a la computación clásica?

☐ Sí

☐ No

4. ¿Consideras que las comunicaciones (redes sociales, paginas web, telefonía celular, mensajería instantánea, etc.) actualmente son seguras?

☐ Sí

☐ No

5. ¿Conoces algún algoritmo de encriptación tradicional?

☐ Sí

☐ No

6. ¿Puedes nombrar alguno de ellos?

Escribe tu respuesta

7. ¿Cuales son los avances más recientes en encriptación usando la computación cuántica?

☐ Criptografía cuántica de clave pública

☐ Criptografía basada en lattices

☐ Criptografía post-cuántica

☐ Comunicación cuántica segura

☐ Otras

8. ¿Conoces las normativas aplicadas a seguridad informática tales como: el Reglamento General de Protección de Datos (RGPD) o la Directiva NIS (Network and Information Security) de la Unión Europea.?

☐ Sí

☐ No

9. ¿En el mediano y largo plazo crees que los algoritmos de encriptación tradicionales dejaran de funcionar?

☐ Sí

☐ No

☐ Otras

10. La Inteligencia Artificial juega un papel muy importante dentro de la seguridad de las personas dado que a diario compartimos mucha información con entidades que son operadas por IA. ¿Crees que en algún momento toda esta información pueda perjudicarnos? Menciona un ejemplo.

☐ Sí

☐ No

☐ Otras

Diseños muestrales

Tamaño y calidad de la muestra

Universo: *Profesionales de la computación que tienen experiencia en el ramo de TI*

Muestra:

Grupo 1: *8 profesionales de la información que tienen experiencia en el ramo de la seguridad informática.*

Grupo 2: *8 profesionales de la información que tienen experiencia en el ramo de la computación cuántica.*

Demostración de la aplicación

Se aplicaron las encuestas a los 2 grupos de individuo que tienen experiencia en tecnologías informáticas con acento en ciberseguridad y computación cuántica y personas con poca o nula experiencia en tecnologías informáticas con acento en seguridad informática y computación cuántica.

La Computación Cuántica, Ciberseguridad e Inteligencia Artificial Hoy En Día

<https://forms.office.com/r/dXHUgmESgJ>

Encuestas aplicadas:



Encuesta 1.pdf



Encuesta 2.pdf



Encuesta 3.pdf

Análisis de resultados y conclusiones

Tras las encuestas al universo de personas se determinaron los siguientes datos

La Computación Cuántica, Ciberseguridad e Inteligencia Artificial Hoy En Día

17

Respuestas

04:01

Tiempo promedio para finalizar

Activo

Estado

[Ver resultados](#)

 [Abrir en Excel](#) ...

1. ¿Hace cuanto tomaste algún curso/taller/diplomado referente a seguridad informática?

[Más detalles](#)

 Información

 Nunca	6
 1 o 2 años	8
 3 o 4 años	0
 + 5 años	3



*Dato de la Actividad 1.

2. ¿Hace cuanto tomaste algún curso/taller/diplomado referente a computación cuántica?

[Más detalles](#)

 Información

 Nunca	16
 1 o 2 años	1
 3 o 4 años	0
 + 5 años	0



3. ¿Crees que la computación cuántica llegue a desplazar a la computación clásica?

[Más detalles](#)

 Información

 Sí	8
 No	7



4. ¿Consideras que las comunicaciones (redes sociales, paginas web, telefonía celular, mensajería instantánea, etc.) actualmente son seguras?

[Más detalles](#)

● Sí	1
● No	16



5. ¿Conoces algún algoritmo de encriptación tradicional?

[Más detalles](#)

Información

● Sí	7
● No	10



6. ¿Puedes nombrar alguno de ellos?

[Más detalles](#)

 Información

8

Respuestas

Respuestas más recientes






1 encuestados (13%) respondieron **AES Advanced Encryption Standard** para esta pregunta. ...

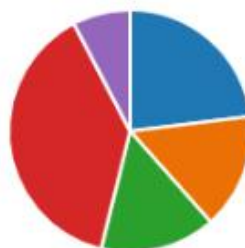
RSA
AES Advanced Encryption Standard
Simetrico SSL Simétrico

7. ¿Cuales son los avances más recientes en encriptación usando la computación cuántica?

[Más detalles](#)

 Información

	Criptografía cuántica de clave p...	3
	Criptografía basada en lattices	2
	Criptografía post-cuántica	2
	Comunicación cuántica segura	5
	Otras	1



8. ¿Conoces las normativas aplicadas a seguridad informática tales como: el Reglamento General de Protección de Datos (RGPD) o la Directiva NIS (Network and Information Security) de la Unión Europea.?

[Más detalles](#)

 Información

	Sí	2
	No	15



9. ¿En el mediano y largo plazo crees que los algoritmos de encriptación tradicionales dejarán de funcionar?

[Más detalles](#)

 Información


	Sí	10
	No	5
	Otras	0



10. La Inteligencia Artificial juega un papel muy importante dentro de la seguridad de las personas dado que a diario compartimos mucha información con entidades que son operadas por IA. ¿Crees que en algún momento toda esta información pueda perjudicarnos? Menciona un ejemplo.

[Más detalles](#)

 Información

	Sí	12
	No	2
	Otras	3



CONCLUSIÓN

En conclusión, la combinación de la encriptación tradicional y la computación cuántica plantea tanto desafíos como oportunidades en términos de seguridad de la información. Si bien los sistemas de encriptación tradicionales pueden volverse vulnerables a los ataques cuánticos, la encriptación cuántica surge como una posible solución que aprovecha los principios de la mecánica cuántica para proporcionar una seguridad más robusta.

La investigación en este campo se centra en el desarrollo de algoritmos y protocolos de encriptación cuántica que sean resistentes a los ataques cuánticos. Sin embargo, la implementación práctica de estos métodos plantea desafíos en términos de compatibilidad con los sistemas existentes y la escalabilidad.

A medida que avanza la investigación, es importante seguir explorando y mejorando los métodos de encriptación cuántica para garantizar la seguridad de la información en un entorno de computación cuántica en constante evolución.

Además, se requiere una mayor colaboración y discusión entre expertos en criptografía, computación cuántica y seguridad de la información para abordar de manera efectiva los desafíos planteados.

En resumen, la combinación de la encriptación tradicional y la computación cuántica plantea desafíos y oportunidades en la seguridad de la información. La encriptación cuántica ofrece un enfoque prometedor para garantizar una mayor seguridad, pero es necesario continuar investigando y superando los desafíos asociados para su implementación práctica efectiva.

BIBLIOGRAFÍA

Shor, P. W. (1994). Algorithms for quantum computation: Discrete logarithms and factoring. En Proceedings of the Annual Symposium on Foundations of Computer Science (FOCS) (pp. 124-134). IEEE.

Gisin, N., Ribordy, G., Tittel, W., & Zbinden, H. (2002). Quantum cryptography. Reviews of Modern Physics, 74(1), 145-195.

Preskill, J. (2018). Quantum Computing in the NISQ era and beyond. Quantum, 2, 79.

Bernstein, D., & Buchmann, J. (1996). Post-quantum cryptography. Springer-Verlag Berlin Heidelberg.

Nielsen, M. A., & Chuang, I. L. (2010). Quantum computation and quantum information. Cambridge University Press.

Lütkenhaus, N., & Shields, A. J. (2017). Quantum cryptography: From theory to practice. Cambridge University Press.

Boneh, D., & Shor, P. (2013). Cryptography in the age of quantum computers. Notices of the American Mathematical Society, 60(5), 688-697.

Ding, J., Gao, F., & Long, G. (2017). Quantum secure direct communication and authentication. Springer.