International Journal of Engineering Research and Technology. ISSN 0974-3154, Volume 14, Number 7 (2021), pp. 593-600

The Imminent Obsolescence of Cryptographic Algorithms and the Arrival of Quantum Computation

Diana Milena Rodríguez Herrera[1], Jhoan Manuel Patiño Fandiño[2], Norberto Novoa Torres[3]

[1,2]Engineers, Universidad Distrital Francisco José de Caldas, Technology Department, Bogotá Colombia. Email: dimrodriguezh@correo.udistrital.edu.co, jmpatinof@correo.udistrital.edu.co

[3]Magister in education, Teaching staff, Universidad Distrital Francisco José de Caldas, Technology Department, Bogotá Colombia. Email: nnovoat@udistrital.edu.co

Abstract

This article discusses how the forthcoming use of quantum computing could affect information security, which is currently protected with the use of symmetric and asymmetric cryptographic algorithms. Initially, an explanation of some algorithms currently implemented in different virtual environments will be given, followed by an introduction to quantum computing, and finally an analysis of the impact that quantum computers might have in the field of cybersecurity will be carried out.

Keywords: Cryptology, quantum computing, cryptographic algorithms, symmetric algorithms.

I.INTRODUCTION

Given the constant flow of sensitive information on the web, public and private organizations find themselves in need of better security protocols. Different cryptographic algorithms that use mathematical concepts have been created and implemented in order to encrypt the information that is transmitted and thus ensure authentication, confidentiality, integrity, and availability of the data [1].

Depending on the algorithm used, it may take a certain time for a common computer to decrypt the key of an information system. The objective of this article is to determine how quantum computing and the arrival of quantum and post-quantum algorithms would reduce the time decryption takes; AES, 3DES and RSA are some of the encryption algorithms that could become obsolete with the commercialization of quantum computers.

II. HISTORY OF CRYPTOGRAPHY

Cryptography was initially based in transposition and substitution ciphers, changing the position of the letters of the alphabet to send secret messages, and early records of Egyptians using this ciphers more than 4 thousand years ago have been found [2]; the most representative example of such protocols is the scytale, used by Spartan ephors to send secret messages using two wooden sticks and a strip of leather or papyrus that, when rolled into them, showed a hidden message, as seen in Figure 1.

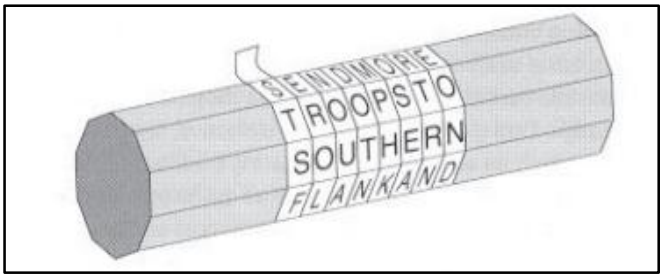

Fig. 1. Scytale [3]

World War II introduced cryptographic mechanisms that allowed the transfer of hidden information, such as the Enigma machine created by the Germans. At the same time scientist and mathematician Alan Turing developed the Turing machine, capable of deciphering messages created by the Enigma, kicking off computing development, and marking the beginning of modern cryptography [4].

In the 1960s the development of Public Key Cryptography set a precedent; before that encryption was exclusively symmetric, and used the same key to encrypt and decrypt the information. And thus asymmetric cryptography, which implemented the use of two keys (public and private) was born [5].

III. SYMMETRIC ENCRYPTION

Also known as secret key encryption, in which both sender and receiver agree on a single key to transmit a message (called plaintext); the encryption algorithm produces intelligible data about the same length of text as said plaintext. The decryption process is the inverse of the encryption and uses the same encryption key.

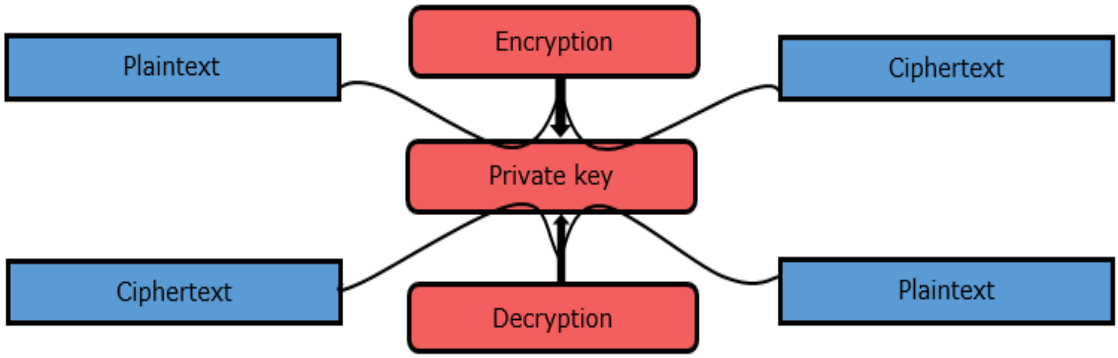

Fig. 2. symmetric encryption

In the symmetric algorithm example [6], Alice and Bob have identical keys for the same padlock. These keys are exchanged before sending the secret message. Alice writes the message and keeps it in a box, which she locks with her key; she then sends Bob the box. The message is secure inside the box while it travels through the postal mail system. When Bob receives the box, he uses his key to unlock the box and see the message. Bob can use the same box and padlock to send another secret message to Alice.

III.I 3DES encryption algorithm

This algorithm comes from the DES algorithm; designed by IBM and published in 1975, it was initially used in financial institutions. It is currently one of the most widely used algorithms in credit cards and other electronic means of payment; however, it is slowly disappearing because its encryption process tends to be relatively slow, and is being replaced by the AES algorithm, from which no vulnerabilities have been discovered to date [7].

The DES algorithm is a sequence of data bit permutations and substitutions combined with an encryption key. The key and the algorithm are used to encrypt and decrypt. The key has a block size of 64 bits, 8 of which are used for checking parity and 56 for encryption. The least significant bit of each byte of the key is used to ensure odd parity. DES uses the XOR operator with the following truth table:

1 XOR 1 = 0

1 XOR 0 = 1

0 XOR 1 = 1

0 XOR 0 = 0

The 3DES algorithm applies the DES algorithm three times to the same plaintext block; the first time encrypting it using the first 56-bit key (k1), then the data is decrypted using the second 56-bit key (k2), and finally the data is again encrypted with the third 56-bit key (k3) [6].

Table 1. 3DES algorithm features

3DES algorithm	
Official name	Triple Data Encryption Algorithm
First published	1977 (DES)
Encryption	Symmetric
Key length	112-bit and 168-bit
Speed	Slow
Time to break it (assuming the computer can test 255 keys per second)	4.6 thousand million years, with current technology
Memory usage	Medium

Source: Cisco

III.II AES block cipher

AES (Advanced Encryption Standard) is an encryption algorithm that arises after the decay of its predecessor, DES; the NIST (National Institute of Standards and Technology) opened a competition for any person or corporation that wanted to create a new encryption algorithm. After three years of validation and testing, the Rijndael algorithm (AES) was the winner in October, 2000. This algorithm works by encrypting and decrypting each data block, using the same private key for both processes [8].

The Rijndael algorithm is an iterative block cipher, that is, the encryption key and some of its initial input blocks are replaced by specific outputs, and others shuffle some of their bits around.

The algorithm uses different blocks sizes and key lengths. Keys increase by 64 bits (128,192, 256 bits) and encrypt data blocks of the same size.

Table 2. AES features

AES block cipher	
Official name	Advanced Encryption Standard
First standardized	2001
Encryption	Symmetric
Key length	128, 192 and 256
Speed	High
Time to break it (assuming the computer can test 255 keys per second)	149 trillion years
Memory usage	Low

Source: Cisco

IV. ASYMMETRIC ENCRYPTION

Asymmetric encryption works with two types of keys; A public key that the sender uses to encrypt the message to be sent, and a private key which is used if and only if the receiver wishes to decrypt the message. It should be noted that this private key is only available to the receiver, who is also the one who provides the public keys that encrypt messages. This ensures control of the keys and makes it easier to identify each sender, since each public key is unique.

Disadvantages

- Similar key and message lengths require more processing time.
- Keys must be larger than in symmetric encryption.
- The encrypted message takes up more space than the original.

IV.I RSA Algorithm

Designed by Ron Rivest, Adi Shamir and Leonard Adleman in 1978, the RSA is an asymmetric algorithm for Public Key Encryption. Its security is based on the difficulty of factoring large numbers. Both public and private keys are calculated from a number that is obtained as a product of two large primes. It is widely used in e-commerce protocols. Since its discovery no one has managed to break its safety, and it is considered one of the safest asymmetric algorithms. When attempting to break it, the attacker will face a factoring problem or discrete logarithm if they want to retrieve plaintext from the cryptogram and public key [9].

According to Cacuango [10] RSA is known for the initials of its 3 developers (Rivest, Shamir and Adleman). It is said that this algorithm has resisted all attempts to break it for more than a quarter of a century; it is considered a very robust cryptosystem. The algorithm uses two large prime numbers *p* and *q* to generate public and private keys; for encryption and decryption purposes *p* and *q* must be different. The sender encrypts the message using the receiver's public key and when the message is transmitted, the receiver can decrypt it using their own private key [11-12].

Its main disadvantage is that it requires keys of at least 1024 bits to guarantee greater security, compared to 128 bits for symmetric key algorithms, which makes it relatively slow. RSA operations can be broken down into three steps; key generation, encryption and decryption.

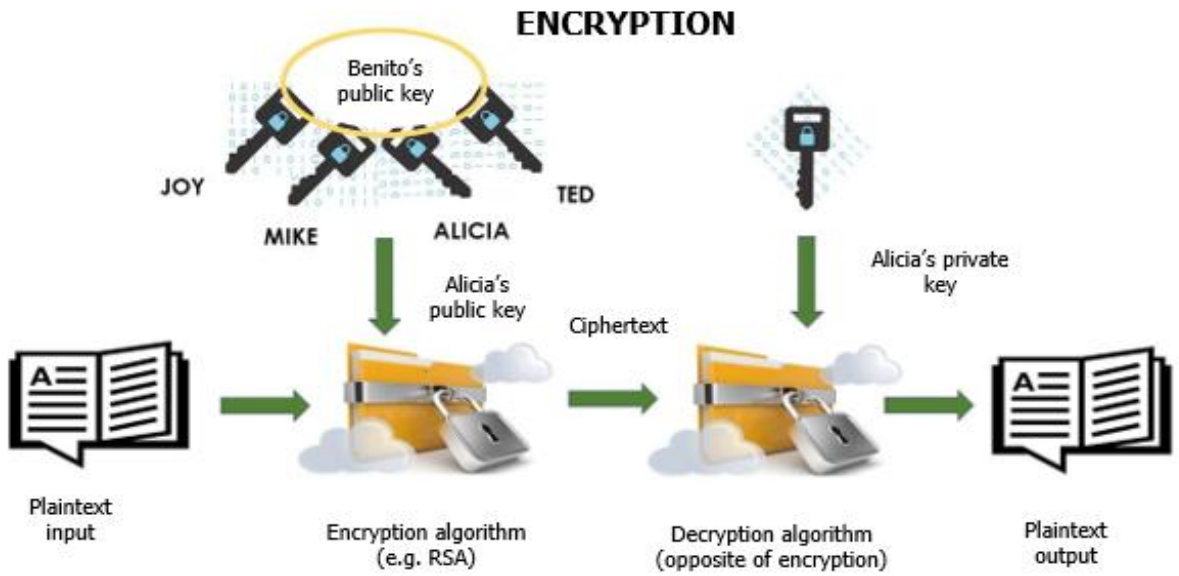

Fig 3. Asymmetric encryption security.

IV.I.I Key generation procedure [13].

1. Choose two different large random primes p & q such that $p \neq q$.
2. Compute $n = p \times q$.
3. Compute: phi (n) = (p-1) (q-1).
4. Choose an integer e such that 1 <e <phi (n)
5. Determine d such that $d \times e = 1$

   mod phi (n); d is kept as private key.
6. Public key is (n, e) and the private key is (n, d). Keep d, p, q, and phi values secret.

IV.I.II Encryption

Plaintext P <n

Ciphertext: $C = P^e \ mod \ n$

IV.I.III Decryption

Ciphertext: C

Plaintext: $P = C^d \ mod \ n$

V. ALGORITHM COMPLEXITY

The mathematical complexity provides a basis to analyze the requirements that cryptanalytic techniques must satisfy, and to study the difficulties inherent in both symmetric and asymmetric encryption systems, such as those previously mentioned. The vulnerability of a cryptosystem is determined by the complexity of the algorithms used to decipher it. Said complexity is determined by the time they take, and the space they use in memory [14]**.**

Currently, classical computers have limited computational capacity, and the security of cryptographic algorithms is based on the fact that this computing power is limited [15], so trying to break certain algorithms is a task that is not within their capacity. With the arrival of quantum computing, which has evolved over the years, post-quantum algorithms and high processing speeds are introduced, the latter being unlimited. This is why the complexity of classical algorithms will be obsolete in the near future.

VI. INTRODUCTION TO QUANTUM COMPUTING

To conceptualize quantum computing it is necessary to conceptualize classical computing. Computing is determined by a binary system, where the minimum unit of information is the bit; the bit can have two states: 1 or 0. These states are unique and cannot take another value, since the bits are translated as absence of voltage (0) and presence of voltage (1) in a circuit. Unlike classical computing, quantum computing's minimum unit (qubit or quantum bit) is represented by a particle (Figure 1). It follows the laws of quantum mechanics, which means it can take a state 1, a state 0, or both states at the same time [16]; It can also be the case where the qubit is more inclined towards a state within said particle.

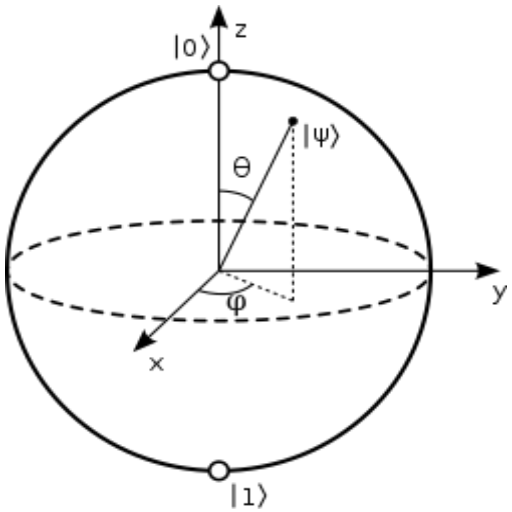

Fig. 4. Qubit graphical representation.

In classical computing laws, having three bits represents eight states or possible combinations {000,001,011,111,101,110,100,010}. Thanks to quantum superposition, having 3 qubits represents the same eight states simultaneously in an instant of time. Qubits are also correlated with each other, meaning that the value of one may depend on the value of another, which is known as quantum entanglement. Google, IBM and Microsoft are companies that currently design quantum hardware, already achieving entanglement with several dozen qubits [17].

VI.I Quantum superposition

The famous thought experiment of Schrödinger's cat, made by Erwin Schrödinger in 1937 explains how quantum superposition works [18]; imagine a cat inside a box, a glass bottle that contains poison and a hammer that breaks the bottle when it perceives an alpha particle are next to it. the particle is emitted by a radioactive atom near the hammer's sensor, with a 50% chance of being emitted and a 50% chance of decaying. One hour later there is a chance the particle was emitted and the cat is dead, or that it decayed and the cat is alive. During this time the cat is in ***superposition****;* that is to say, the cat is alive and dead at the same time (it has two states simultaneously) within the box. When the box is opened the superposition brakes and the cat is in a single state, either alive or dead.

VI.II quantum entanglement

Quantum entanglement is an essential feature of quantum computation; It occurs when two particles interact in a way such that it is impossible to know their individual states, as it was proposed by Albert Einstein, Boris Podolsky and Nathan

Rosen in the *Physical Review* magazine in 1935, and initially called EPR paradox [19]. It occurs when the quantum particle ***a*** influences the state of another particle ***b***, regardless of the distance between, sometimes millions of light years; Einstein called this phenomenon "ghostly action at a distance."

That is, the particle a contains different states called *w* and *x* and the particle **b** contains the states *y* and *z*, and these can be at a considerable distance. Consequently, it can be said that when any state, in this case state (x) of the particle **a** changes, the state (z) of the particle **b** changes too, and vice versa.

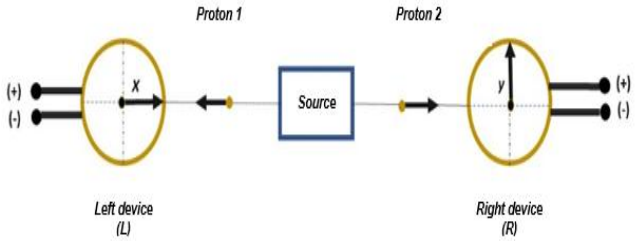

Fig 5. Quantum entanglement.

VI.III Quantum Computer

Quantum computing began to develop in the eighties as a result of the proposals of Deutsh and Feymann, who suggested using quantum systems as a calculation tool; but it was not until 1994 when P. Shor [20-21] reached an important milestone in quantum computing with polynomial-time algorithms used for factoring integers and discrete logarithm calculation, giving quantum computers the possibility to break public key cryptosystems.

D-Wave Systems is the developer of the most powerful quantum computers created since 2009, with the creation of its first commercial quantum computer with 6 qubits. Then, in 2011 they created the D-Wave One, with a capacity of 128 qubits, and in 2013 they went as far as 512 qubits with the D-Wave Two. The D-Wave 2X, a model launched in 2015, had a capacity of 1000 qubits, and in 2017 they reached more than 2000 qubits with the D-Wave 2000Q. D-Wave Systems works with companies such as internet giant Google and NASA [22], where they implemented the p16 prototype with up to 5460 qubits. Even so, these super computers have not been able to perform processes that a classic computer cannot do.

IBM and Google have their own 54-qubit quantum computers with a Sycamore processor, and the Q System with 50 qubits. These computers have different purposes and applications; they can run financial models, as well as quantum simulations for medical breakthroughs and artificial intelligence.

VII. QUANTUM ALGORITHMS

Quantum algorithms are developed from the need to overcome the limits of classical mechanics, making use of quantum mechanics to solve problems that over time classical computing will not be able to solve. Two of the most important algorithms for quantum computing are the Shor's algorithm [23] and the Grover's algorithm, both capable of processing large amounts of information in a short time period.

VII.I Shor's algorithm

Created by Peter Shor in 1994, this algorithm demonstrates an exponential reduction in the time of integer factorization; given an integer $N \in Z \geq 0$, the algorithm tries to find the only decomposition in prime factors that guarantees the Fundamental Theorem of Arithmetic. In practice, an IBM quantum computing team led by Isaac Chuang succeeded in factoring the number 15, the smallest number that validates Shor's algorithm, into its factors 3 and 5 using a 7-qubit quantum computer. Then, in March 2016, Chuang, along with a group of researchers from MIT managed to create a 5-qubit quantum computer that could also run Shor's algorithm to factor the number 15 with 99% accuracy [24].

Taking into account that classical computers cannot efficiently solve the factoring hypothesis, which is a fundamental piece of modern cryptography, quantum computing makes this hypothesis solvable as there is an exponential improvement comparing the quantum model versus the classic [25].

VII.II Grover's algorithm

Created by Lov Kumar Grover in 1996, this algorithm solves the problem of finding an element or a set of elements within an unordered list of N elements. A simple example is looking for a card within a deck such that the solution to the problem is only $M < N$ elements. The computational complexity to perform the search in classical computing is $O(N)$ since it requires N checks of the operation to find the element; the Grover's algorithm (also called unstructured search) allows to speed up the process and achieves a complexity of $O(\sqrt{N})$ obtaining a quadratic improvement of the process [26].

This algorithm is known for its direct implications regarding the vulnerability of current cryptology, as it focuses on heavy searches for items in unordered lists. An example in cybersecurity is having an RSA-encrypted list of stored passwords that an intruder tries to obtain by means of a brute-force attack. To obtain the list in classical computing it would require an average of $N/2$ comparisons; with the Grover's algorithm and quantum superposition, time would be considerably reduced to $\sqrt{N}$ [27].

VIII. POST-QUANTUM ALGORITHMS

Post-quantum algorithms arise from the need to develop asymmetric algorithms that are based on demonstrable mathematical problems for quantum computing. Post-quantum multivariate cryptography, lattice-based, and code-based cryptography are the biggest advances so far.

VIII.I Multivariate cryptography

This cryptography is based on the problems associated to nonlinear system equations in *n* variables on finite fields. Normally a user faces the challenge to decipher, authenticate or digitally sign when *x* polynomials (*p1, ..., px)* , of variable *n* and degree *d*, usually *(d=2)* are exposed to a finite field *F* with *z = (z1, ..., zx)* ∈ F^x, and they must find w = (w1,….w*n*) for the associated system,

$$\{P\_1\ (w\_1, \dots, w\_(n) =)\ z\_1\ \ P\_2\ (w\_1, \dots, w\_(n) =)\ z\_2\ \dots P\_m\ (w\_1, \dots, w\_(n) =)\ z\_m$$

This cryptography allows the creation of schemes such as the QUARTZ encryption algorithm [28] that creates 100-bit signatures, or the ZHFE encryption scheme [29], which is one of the few promising candidates for a multivariate public key encryption algorithm. It is also possible to incorporate said schemes into different platforms.

VIII.II Code-based cryptography

When a message is to be sent, it is interpreted in bits that can be altered or contain errors due to problems in the communication channel, in the network, noise or others. This means that the message does not arrive with its initial integrity, hence the importance of correcting errors based on information redundancy. An example is repeating messages (bits), that is, if it is required to send 1 bit the receiver will get eight 8 possible bit combinations (111,000, and its different combinations) three times, but the correct value will be the one that gets the most occurrences.

Code-based cryptography for post-quantum computing is based on the *NP-complete* problems; The Coset Weights, where the input is a binary matrix *H*, a binary vector *S*, a nonnegative integer *W*, and its property contains a vector *e* of *Hamming* weight less than *W*, such that S = eH, and Subspace Weights where the input is the same binary matrix and nonnegative integer as the previous problem, and its property contains a vector *x* of *Hamming W* such that xH = 0 [30].

IX. CYBERATTACKS

The objective of cyberattacks is to search for vulnerabilities in an information system in order to access, steal or manipulate it, using different techniques and algorithms designed for this. An attack is made in order to obtain some kind of monetary, political or social gain [31].

It is said that a cyberattack occurs when it compromises any of these factors:

- **Availability**: Being able to access the resources or services of a computer system when required. It is generally affected when, through a Denial of Service attack (DoS), the server is saturated with multiple requests, preventing the user from accessing.
- **Confidentiality:** Keeping sensitive information safe using protocols and encryption, in order to guarantee privacy and restrict access to unauthorized users. It is violated when an intruder gains access to the system and manages to view this information [32].
- **Integrity:** It is in charge of preserving all the information, preventing intruders from affecting or modifying it, generating inconsistencies or radical changes in an information system. Intruders usually make use of techniques that break communication protocols, accessing and altering information [33].

IX.I Cryptanalysis

It is a set of techniques and methods to evaluate the security of a cryptosystem. It usually starts with a study of strategies aimed to find weaknesses that could be used to break a given cryptosystem [34].

When the encryption and decryption algorithms are known, the most elementary attack is the brute-force attack, which consists of exploring all the possible keys to break the cryptographic system. It is an easy job when the key size is small; it will take longer and in some cases be impossible if the key size is very large. Thus, it is essential that the key space be as large as possible in the cryptosystem [35].

X. IMPACT

The level of processing in quantum computing is superior to classical computing. RSA, AES and 3DES algorithms can be breached in less time than Grove's and Shor's algorithms because, when using qubits and making use of the properties of quantum computing, the processing speed is greater than the speed you get using bits in classical computing.

If Grove's algorithm is used in classical computing, its notation would be $\mathbf{o(\frac{n}{2})}$ and in quantum computing it is $\mathbf{o(\sqrt{n})}$, which means higher processing speed in quantum computing. When comparing the RSA, AES and 3DES algorithms, the difference in processing speeds can be observed.

Table 3. Algorithm comparison (RSA, 3DES, AES)

Algorithm	Key Size	Classic impact	Quantum impact
RSA	2048-bit	Up to 2^4096 2^n in qubits	Up to 4096 qubits
3DES	2048-bit	Search: 1024 bits	Search: 45 qubits
AES	128-bit	Time: 10.76 quadrillion years 128-bit security	Time: 6 months 64-qubit security

Currently, public keys are insecure considering they are based on number theory (discrete logarithms in cyclic groups, factorization, etc.). This means that RSA-based schemes

(signature or key encryption) will be considered obsolete due to the computational capacity of the quantum computing and the use of post-quantum algorithms.

XI. CONCLUSIONS

- Quantum algorithms have the ability to process data faster due to the use of qubits, while classical asymmetric encryption algorithms handle classical encoding with the use of bits. These can have only two states and not multiple like qubits, reducing the processing capacity.
- Post-quantum cryptography arises from the need to solve mathematical problems based on the most efficient quantum algorithms (Shor's and Grove's), and will lead to optimizing and streamlining processes, making them useful tools in technology.
- As a consequence, quantum algorithms allow the information of a system to be protected with greater security, since their algorithmic complexity allows them to be less vulnerable to cyberattacks and in turn become a reliable protocol as the size of their keys increases.

REFERENCES

[1] SHEIKH, Mohammed Firdos Alam, et al. A Study on Performance Evaluation of Cryptographic Algorithm. retrieved from Emerging Trends in Expert Applications and Security. Springer, Singapore, 2019. p. 379-384.

[2] Xifré Solana, P. (2009). Antecedentes y perspectivas de estudio en historia de la Criptografía (Bachelor's thesis).

[3] Delgado Vargas, Kevin Andrae, De Abiega L'Eglisse, Alfonso Francisco, Gallegos-Garcia, Gina & Cabarcas, Daniel (2019). Un acercamiento a la línea del tiempo de los algoritmos criptográficos. Revista Digital Universitaria (rdu). Vol. 20, no. 5, September-October. doi: http://doi.org/10.22201/codeic.16076079e.2019.v20n5.a7.

[4] Singh, S. (2000). » The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography «, 1st.

[5] Menezes, A. J., Van Oorschot, P. C., & Vanstone, S. A. (2018). Handbook of applied cryptography. CRC press.

[6] Ariansen, R., & Rojas, J. (2017). Implementacion de Protocolo de Cifrado TLS para mejorar la Seguridad de la capa de Transporte. Chiclayo: Universidad Señor de Sipan.

[7] Camacho Reina, G. A. (2019). Análisis de tecnologías criptográficas, 3DES y RSA, basado en las Normas ISO 27001, para garantizar la integridad de datos en la capa de Transporte con dispositivos Raspberry PI (Master's thesis, Quito).

[8] Muñoz, A. M. (2004). Seguridad europea para EEUU–Algoritmo Criptográfico Rijndael. Madrid, September 2017

[9] López, M. J. L. (2011). Criptografia y seguridad en computadores (pp. 4-0). Universidad de Jaén, Versión.

[10] Cacuango Lagla, S. E. (2019). Evaluación de una Red LAN para el establecimiento de las Políticas de la Calidad de Servicio (Master's thesis, Quito).

[11] Kumar, A., Jakhar, S., & Makkar, S. (2012). Comparative Analysis between DES and RSA Algorithm's. International Journal of Advanced Research in Computer Science and Software Engineering, 2(7), 386-391.

[12] Zhou, X., & Tang, X. (2011, August). Research and implementation of RSA algorithm for encryption and decryption. In Proceedings of 2011 6th international forum on strategic technology (Vol. 2, pp. 1118-1121). IEEE.

[13] Singh, G. (2013). A study of encryption algorithms (RSA, DES, 3DES and AES) for information security. International Journal of Computer Applications, 67 (19).

[14] Carlos,B. Criptografía, MAPLE y RSA,1998,pp. 1-13

[15] Liu, W., Gao, P., Liu, Z., Chen, H., & Zhang, M. (2019). A quantum-based database query scheme for privacy preservation in cloud environment. Security and Communication Networks, 2019.

[16] Bonillo, V. M. (2013). Principios fundamentales de computación cuántica. Universidad de La Coruña.

[17] Wolf, G. (2019). Mecánica Cuántica y Computación. Software Gurú, (58), 42-43.

[18] Schrödinger, E. (1992). What is life?: With mind and matter and autobiographical sketches. Cambridge University Press.

[19] A. Einstein, B. Podolsky, and N. Rosen. Can quantum-mechanical description of physical reality be considered complete? Phys. Rev., 47:777–780, 1935.

[20] by Lacalle, J. G. L. (2004). Factorización polinomial de números enteros. LA GACETA DE LA RSME, 7, 515-537.

[21] SHOR, P. (1994): "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer". SIAM J.Comp., 26 (5), pp. 1484-1509 (arXiv: quant-ph / 9508027).

[22] Zaparolli, D. (2019, Octubre). La era de los Cubits. Pesquisa. Recuperado de https://revistapesquisa.fapesp.br/

[23] Shor, P. W. (1994, November). Algorithms for quantum computation: discrete logarithms and factoring. In Proceedings 35th annual symposium on foundations of computer science (pp. 124-134). IEEE.

[24] CORDOBA, Diego; MÉNDEZ GARABETTI, Miguel. Criptografía post cuántica. In XIX Workshop de Investigadores en Ciencias de la Computación (WICC 2017, ITBA, Buenos Aires). 2017.

[25] Pastor Díaz, U. (2019). Algoritmos fundamentales en computación cuántica.

[26] López López, M. (2020). Implementación del algoritmo de Grover en los ordenadores cuánticos de IBM.

[27] Gómez, N., Gómez, A., Gómez, A., & Villabona, D. (2019). Arquitectura de la computación cuántica: La información es transmitida más rápido que la velocidad de la luz. Universidad industrial de Santander.

[28] Patarin, J., Courtois, N., & Goubin, L. (2001, April). Quartz, 128-bit long digital signatures. In *Cryptographers' Track at the RSA Conference* (pp. 282-297). Springer, Berlin, Heidelberg.

[29] Porras, J., Baena, J., & Ding, J. (2014, October). ZHFE, a new multivariate public key encryption scheme. In *International workshop on post-quantum cryptography* (pp. 229-245). Springer, Cham.

[30] Reyes Rosado, Á. R. (2018) Estado de la criptografía post-cuántica y simulaciones de algoritmos post-cuánticos. (Master's thesis, Madrid).

[31] Mieres, J. (2009). Ataques informáticos: Debilidades de seguridad comúnmente explotadas. Jan-2009.

[32] Guamán Sinchi, B. V. (2015). Anatomía de un ataque Informático (Bachelor's thesis, Universidad del Azuay).

[33] Aguilar Feijóo, F. J. (2019). Los ataques informáticos y su incidencia en la seguridad de servidores con Sistema Operativo Linux de Entidades de Gobierno Local (Master's thesis, Ecuador).

[34] Orúe, A. B. (2013). Contribución al estudio del criptoanálisis y diseño de los criptosistemas caóticos. (ph.D thesis, Madrid).

[35] Ríos, N. R. T., í lvarez Morales, E. L., & Sandoya, S. D. C. (2017). Seguridad Informática, un mecanismo para salvaguardar la Información de las empresas. Publishing Magazine, 4 (10 (2)), 462-473.