Criptografía

Sarah Bracho ~ Nicolás Patalagua

sarahbracho1703@gmail.com ~ nicopatalagua@gmail.com

Resúmen: *En este documento se realiza una breve introducción a la criptografía, como una herramienta de seguridad informática basada en el principio de garantizar las propiedades de confidencialidad, integridad y disponibilidad de la información.*

Abstract: *This document provides a brief introduction to cryptography as a computer security tool based on the principle of ensuring the properties of confidentiality, integrity and availability of information.*

I. INTRODUCCIÓN A LA CRIPTOGRAFÍA

La criptografía desde la antigüedad está catalogada como un arte, el cual consiste y consistía en escribir mensajes de forma que no puedan ser entendidos o descifrados, sin tener una clave o un método. Actualmente, es de amplio uso en áreas relacionadas no solo con la computación sino también en áreas de economía, política, sociedad, cultura, etc. Es decir en las áreas que requieran seguridad para diversos tipos y fuentes de información.

A nivel social, entre las áreas que integran la criptografía como una medida de seguridad informática están las organizaciones que en las últimas décadas, cuentan con la necesidad de migrar las viejas formas de seguridad de información (Cajas fuertes y clasificación de documentos) por formas que integren tecnología y desarrollo como lo es la introducción de sistemas informáticos. Estos sistemas informáticos han generado un indispensable uso de herramientas de protección de archivos, datos e información almacenada y recolectada en computadores, discos duros, servidores o cualquier otro medio de almacenamiento. Esta necesidad se basa en los pilares de la seguridad de la información *confidencialidad, integridad, disponibilidad* y *autenticación.* [1]

II. DEFINICIÓN DE CRIPTOGRAFÍA

El origen de la palabra criptografía se remonta a una etimología griega *κρύπτος*, que hacía referencia a algo recubierto o oculto, esta palabra está compuesta por las palabras κλυπτος (Kryptos) que significa oculto y el sufijo γραφια (Grafía) que significa grafia. [2]

En el libro *Information Security and Cryptography*, Hans Delfs y Helmut Knebl, definen la criptografía como la ciencia de mantener los secretos en secreto. [3] En una definición más acertada, un grupo de investigadores de la universidad de Zaragoza, la definen como el estudio de algoritmos, protocolos y sistemas que se usan para dotar de seguridad a las comunicaciones, la información y las entidades que se comunican. [4]

Esto da a entender que la criptografía es un conglomerado de técnicas de codificación o cifrado que tienen como objetivo alterar las representaciones lingüísticas (lo que comúnmente en teoría de la comunicación se llama código), de cierta información con el fin de alterarlos y hacerlos ininteligibles a receptores indeseados o no autorizados. [5]

III. OBJETIVOS DE LA CRIPTOGRAFÍA

a. Confidencialidad: La ISO (Organización Internacional de Estandarización) la define como "*garantizar que la información es accesible sólo para aquellos autorizados a tener acceso"*. [6]

b. Integridad: Es la propiedad de la información que hace referencia a mantener los datos libres de modificación no autorizadas, a grandes rasgos es mantener con exactitud la información tal cual fue generada, sin manipularla ni alterarla.[6]

c. Vinculación: Se define como la propiedad de la información que la vincula a una persona o a un sistema de gestión de información criptográfico automatizado.[6]

d. Autenticación: Quiza la propiedad de la información más relevante, encargada de proporcionar los mecanismos que verificación de la identidad del comunicador. [6]

IV. CONCEPTOS DE LA CRIPTOGRAFÍA

La criptografía se clasifica en criptografía clásica y moderna, de la siguiente manera:

Figura 1. Clasificación de la criptografía [1]

Además de esto se puede clasificar la criptografía por el tipo, por los estándares, protocolos, algoritmos, mecanismos y aplicaciones.

Por el tipo:

- Criptografía simétrica o convencional
- Criptografía cuántica

- Criptografía asimétrica o de clave pública
- Criptografía de curva elíptica
- Criptografía híbrida
- Criptografía musical

Por la rama:

- Esteganografía
- Criptoanálisis

Por el mecanismo o método

- Firma digital
- Atbash
- Test de primalidad

Por el estándar y protocolo:

- Especificaciones PKCS
- DSS
- OpenPGP
- SET
- SSH
- SSL
- TLS

Por el algoritmo:

- Advanced Encryption Standard
- ARC4
- Blowfish
- DES
- TripleDES
- CuaimaCrypt
- DSA
- ECDSA
- Enigma
- IDEA
- RSA
- TEA
- XTEA
- ROT13

Por su aplicación:

- Software
- Sistemas de pago
- Voto electrónico

V. HISTORIA DE LA CRIPTOGRAFÍA

La historia de la criptografía se puede remontar al uso de jeroglíficos en el antiguo egipto un poco más de 4500 años. Seguido de esto aparecen métodos de *cifrado por sustitución* como el cifrado *Atbash*, extendido entre los eruditos hebreos del siglo VII antes de cristo. Además de esto los griegos también darán su aporte a la criptografía no sólo con el nombre de esta sino también con el *cifrado de transposición* basada en la *escitala.* [7]

Por su parte el imperio romano, brindaría a la humanidad de manos del gran Cayo Julio César, el famoso *cifrado César,* un método de criptografía militar, que desafortunadamente ha desaparecido. [7]

En la edad media, se haría famosos el *cifrado polialfabético* de León Batista Alberti. El salto principal se daría en la segunda guerra mundial, con la *enigma*, una máquina de rotores electromagnética desarrollada por los alemanes y que seria descifrada en su mayor parte por el padre de la *computación moderna*, el matemático Alan Turing. [8]

Luego de estos avances surge la *criptografía moderna*, desarrollada por el ingeniero eléctrico Claude Shannon el famoso padre de la *criptografía matemática,* en el artículo *Communication Theory of Secrecy Systems.* [9]

Para 1967, se diseña y desarrolla el *intercambio de claves Diffie-Hellman* y los algoritmos de *cifrado simétrico*, basados en una clave criptográfica usada tanto por el remitente como por el destinatario, esto genera el concepto de *clave pública.*

VI. DOCUMENTOS RELACIONADOS

1. M. I. Aziz and S. Akbar, “Introduction to Cryptography,” in *2005 International Conference on Microelectronics*, 2005, pp. 144–147, doi: 10.1109/ICM.2005.1590056.

2. J. L. Massey, “An introduction to contemporary cryptology,” *Proceedings of the IEEE*, vol. 76, no. 5, pp. 533–549, May 1988, doi: 10.1109/5.4440.

3. L. de Melo Silva, R. Araújo, F. L. da Silva, and E. Cerqueira, “A new architecture for secure storage and sharing of health records in the cloud using federated identity attributes,” in *2014 IEEE 16th International Conference on e-Health Networking, Applications and Services (Healthcom)*, 2014, pp. 194–199, doi: 10.1109/HealthCom.2014.7001840.

4. A. A. Hernández, R. C. Isidoro, J. J. F. Romero, and H. H. Esquivel, “Validación de expedientes digitalizados, utilizando firma digital y código QR,” in *2018 IEEE International Autumn Meeting on Power, Electronics and Computing (ROPEC)*, 2018, pp. 1–5, doi: 10.1109/ROPEC.2018.8661376.

5. Y. Wang, B. Zhang, W. Lin, and T. Zhang, “Smart grid information security - a research on standards,” in *2011 International Conference on Advanced Power System Automation and Protection*, 2011, vol. 2, pp. 1188–1194, doi: 10.1109/APAP.2011.6180558.

6. Y. Wang, B. Zhang, W. Lin, and T. Zhang, “Smart grid information security - a research on standards,” in *2011 International Conference on Advanced Power System Automation and Protection*, 2011, vol. 2, pp. 1188–1194, doi: 10.1109/APAP.2011.6180558.

VII. CURSOS

1. Cryptography Fundamentals, Sean Oriyano (IEEE)[10]
2. Security of Information and Communication Networks Part 1, Stamatios V. Kartalopoulos (IEEE)[11]
3. Security of Information and Communication Networks Part 2, Stamatios V. Kartalopoulos (IEEE)[12]
4. OPSEC-based RFID Security: Cryptography, Judith M. Myerson (IEEE Woman)[13]
5. Cryptography I, Dan Boneh (Coursera ~ Stanford)[14]
6. Online Cryptography Course, Dan Boneh (Stanford)[15]
7. Understanding Blockchain Technology: The Bitcoin Case Study, Morgen Peck (IEEE)[16]
8. Introduction to IEEE 802.16, Todor Cooklev (IEEE)[17]

VIII. REFERENCIAS

[1] G. G. Paredes, 3150954, and rn, "Introducción a la Criptografía," *Introduction to the criptography*, Jul. 2006, Accessed: 27-Mar-2020. [Online]. Available: http://ru.tic.unam.mx:8080/xmlui/handle/123456789/1105.

[2] "CRIPTOGRAFÍA," *Etimologías de Chile - Diccionario que explica el origen de las palabras*. http://etimologias.dechile.net/?criptografi.a (accessed Mar. 27, 2020).

[3] H. Delfs and H. Knebl, "Introduction," in *Introduction to Cryptography: Principles and Applications*, H. Delfs and H. Knebl, Eds. Berlin, Heidelberg: Springer, 2015, pp. 1–10.

[4] José Pastor Franco, Miguel Ángel Sarasa López, José Luis Salazar Riaño,"Criptografía digital: fundamentos y aplicaciones",Ed. Prensas Universitarias de Zaragoza, 1998

[5]"RDU Introducción a la Criptografía." http://www.revista.unam.mx/vol.7/num7/art55/int55.htm (accessed Mar. 27, 2020).

[6] A. López, "Home." http://www.iso27000.es/ (accessed Mar. 27, 2020).

[7]ingh, Simon (1999). *The Code Book. The Science of Secrecy from Ancient Egypt to Quantum Cryptography*. New York: Anchor Books. p. 25

[8]"Enigma History." https://www.cryptomuseum.com/crypto/enigma/hist.htm (accessed Mar. 27, 2020).

[9]"Mad Cow Cryptography Page," 13-Oct-2003. https://web.archive.org/web/20031013025142/http://www3.edgenet.net/dcowley/docs.html (accessed Mar. 27, 2020).

[10]"Cryptography Fundamentals." https://ieeexplore.ieee.org/courses/details/EDP455 (accessed Mar. 27, 2020).

[11]"Security of Information and Communication Networks Part 1." https://ieeexplore.ieee.org/courses/details/EDP164 (accessed Mar. 27, 2020).

[12]"Security of Information and Communication Networks Part 2." https://ieeexplore.ieee.org/courses/details/EDP165 (accessed Mar. 27, 2020).

[13]"OPSEC-based RFID Security: Cryptography." https://ieeexplore.ieee.org/courses/details/EDP184 (accessed Mar. 27, 2020).

[14]"Cryptography I," *Coursera*. https://www.coursera.org/learn/crypto (accessed Mar. 27, 2020).

[15]"Online Cryptography Course by Dan Boneh." https://crypto.stanford.edu/~dabo/courses/OnlineCrypto/ (accessed Mar. 27, 2020).

[16]"Understanding Blockchain Technology: The Bitcoin Case Study." https://ieeexplore.ieee.org/courses/details/EDP520 (accessed Mar. 27, 2020).

[17]"Introduction to IEEE 802.16." https://ieeexplore.ieee.org/courses/details/EDP061 (accessed Mar. 27, 2020).