Revista Digital Universitaria
Vol. 20, Núm. 5, septiembre-octubre 2019

Un acercamiento a la línea del tiempo de los algoritmos criptográficos

Kevin Andrae Delgado Vargas, Alfonso Francisco de Abiega L'Eglisse, Gina Gallegos-García y Daniel Cabarcas

Resumen

En la actualidad, el intercambio de información a través de dispositivos con características diversas es un proceso que ha incrementado de manera exagerada, lo que implica la necesidad de preservar diferentes servicios de seguridad en la información que se transmite entre ellos. Dado que el poder de cómputo sigue evolucionado a pasos agigantados, en un futuro cercano las computadoras cuánticas presentarán una gran amenaza, ya que dichas computadoras son capaces de realizar millones de operaciones en paralelo, se comprometerá la integridad de los algoritmos que preservan servicios de seguridad y, como consecuencia, los escenarios en donde son utilizados. En este trabajo, se presenta un acercamiento a la línea del tiempo que mantienen los algoritmos criptográficos, y se discute una lista de desafíos que estarían enfrentando los algoritmos del futuro, también llamados postcuánticos.

Palabras clave: algoritmos postcuánticos, criptografía de clave asimétrica, criptografía de clave simétrica, estandarización de algoritmos, niveles de seguridad.

An approach to the timeline of cryptographic algorithms

Abstract

Nowadays, the exchange of information through devices with different characteristics has increased greatly. This brings the need to preserve different security services in the information transmitted between them. Given that computation power continues evolving rapidly, quantum computers will become a great threat in the near future. Since such computers can perform millions of operations in parallel, they will compromise the integrity of algorithms that preserve such security services and, as a consequence, the scenarios where they are used. In this paper, we present an approach to the timeline that cryptographic algorithms maintain, providing a list of challenges that would be facing the algorithms of the future, the post-quantum algorithms.

Keywords: algorithm standardization, asymmetric key cryptography, symmetric key cryptography, post-quantum algorithms, security levels.

DOI: http://doi.org/10.22201/codeic.16076079e.2019.v20n5.a7

Kevin Andrae Delgado Vargas kdelgadov1200@alumno.ipn.mx

En 2018 se graduó de la carrera de Ingeniería en Computación y en el 2019 egresó de la Especialidad en Seguridad Informática y Tecnologías de la Información, ambas de la de la Escuela Superior de Ingeniería Mecánica y Eléctrica, Unidad Culhuacán del Instituto Politécnico Nacional (IPN). Actualmente es estudiante de la Maestría en Ciencias de la Computación del Centro de Investigación en Computación del IPN. Posee un diploma otorgado por la rama estudiantil del Institute of Electrical and Electronics Engineers (IEEE) en desarrollo sobre Raspberry Pi. Tiene conocimientos sobre programación en Python, C++, MATLAB y Visual Basic. Sus áreas de interés son los dispositivos empotrados y el desempeño de mecanismos de encapsulación de llave postcuánticos en dichos dispositivos.

Alfonso Francisco de Abiega L'Eglisse alfonso.deabiega@gmail.com

En 2009 obtuvo el título de Ingeniero en Telemática por el Instituto Tecnológico Autónomo de México. Desde el 2019 posee el grado de Maestría en Ingeniería en Seguridad y Tecnologías de la Información y actualmente es estudiante de Doctorado en Ciencias; ambos en la Escuela Superior de Ingeniería Mecánica y Eléctrica Unidad Culhuacán del IPN. Sus áreas de interés son los dispositivos con recurso limitado y el desempeño de firmas digitales postcuánticas en dichos dispositivos.

Gina Gallegos-García ggallegosg@ipn.mx

Es Ingeniero en Computación y obtuvo el grado de Maestría y Doctorado en Ciencias, todos en la Escuela Superior de Ingeniería Mecánica y Eléctrica (ESIME) Unidad Culhuacan del IPN, en 2003, 2005 y 2011, respectivamente. Durante el verano del 2011, realizó una estancia posdoctoral en la Universidad de Yale, Estados Unidos. De enero de 2010 a marzo del 2019 fue profesora de la sección de estudios de posgrado e investigación y del Departamento de Computación de la ESIME Culhuacan del IPN. Desde abril del 2019 es profesora investigadora del Centro de Investigación en Computación del IPN, en donde es miembro del Laboratorio de Ciberseguridad. Posee la distinción del nivel 1 del Sistema Nacional de Investigadores. Ha sido partícipe de proyectos vinculados con la industria; su desarrollo tecnológico es utilizado en diversas organizaciones, entre las que destacan el SAT, la SDNA, el INE y el IECM, por mencionar algunas. Es miembro de diversas redes de investigación tanto internas como externas al IPN. Entre sus áreas de interés se encuentran la criptografía, los protocolos criptográficos, los dispositivos con recurso limitado, la seguridad demostrable y la votación electrónica.

Daniel Cabarcas dcabarc@unal.edu.co

Es egresado de la Universidad Nacional de Colombia Sede Medellín en la carrera de Ingeniería en Sistemas e Informática. Tiene el grado de Maestría y Doctorado en Ciencias Matemáticas por parte de la Universidad de Cincinnati. De 2011 al 2013 realizó una estancia posdoctoral en la Universidad de Darmstadt. Actualmente, es Investigador Jr. de la Universidad Nacional de Colombia, sede Medellín. Ha dirigido diversas tesis en programas de posgrado y ha publicado varios artículos en revistas científicas, así como en congresos nacionales e internacionales. Sus áreas de interés son la computación algebraica, criptografía y la seguridad informática, por mencionar algunas.

Introducción

En los últimos años, el uso de la tecnología para enviar y recibir información se ha incrementado en la vida cotidiana de niños, jóvenes y adultos. De la mano de estas tecnologías viene el incremento del poder de cómputo, el cual puede utilizarse para atacar o para brindar seguridad a la información.

Históricamente hablando, la criptografía puede clasificarse en: clásica, moderna, cuántica y postcuántica. Pero independientemente de esta clasificación, en la actualidad se define como una ciencia que ha jugado un papel muy importante al dedicar sus esfuerzos a preservar los diferentes servicios de seguridad de la información: confidencialidad, integridad, autenticación y no repudio (Menezes, Van Oorschot, Vanstone y Rosen, 1997), mediante el uso de algoritmos conocidos como criptográficos.

La llegada de un nuevo paradigma de cómputo ha hecho que la computación cuántica, que posee poder de cómputo ilimitado y aspectos relacionados con la física, presente una amenaza inminente para los algoritmos criptográficos que actualmente se consideran seguros (Hallgren, Vollmer, 2009). Como consecuencia, se han presentado recientes necesidades frente al diseño de nuevos algoritmos criptográficos y de su estandarización.

Como consecuencia de ello, el Instituto Nacional de Estándares y Tecnología (NIST, del inglés National Institute of Standards and Technology) en 2017 empezó un proceso de solicitud, evaluación y estandarización de varios algoritmos criptográficos resistentes a ataques efectuados por computadoras cuánticas. Dicho proceso está compuesto de múltiples rondas de evaluación, y tendrá duración de tres a cinco años. A la fecha, ya se tienen resultados de la segunda ronda de evaluación, en la que quedan sólo 26 algoritmos concursantes, a la espera de una nueva eliminatoria (NIST, 2018b).

La línea del tiempo de la criptografía

La criptografía tuvo sus inicios aproximadamente hace más de cuatro mil años, con el primer registro de la escritura egipcia. En aquel entonces, las sustituciones y las permutaciones eran muy utilizadas para transformar la información (Solana, 2009). Ejemplo de este tipo de transformaciones es la escítala de los espartanos o la escritura de algunas civilizaciones como los egipcios o los babilonios (Iashchenko, 2002, ver figura 1).

Figura 1. Escítala espartana.

La Segunda Guerra Mundial marcó un parteaguas para la criptografía, ya que en aquellos años se dieron agigantados avances, dando pie al desarrollo de máquinas mecánicas y electromagnéticas para la protección de la información. Ejemplo de ello se observa en el diseño de la máquina Enigma por parte de los alemanes (Singh, 2000, ver figura 2). A la par, el científico y matemático inglés Alan Turing fue capaz de desarrollar una máquina para descifrar los mensajes creados por la máquina Enigma, dando inicio al desarrollo de las computadoras, marcando una nueva era, la de la criptografía moderna (Singh, 2000).

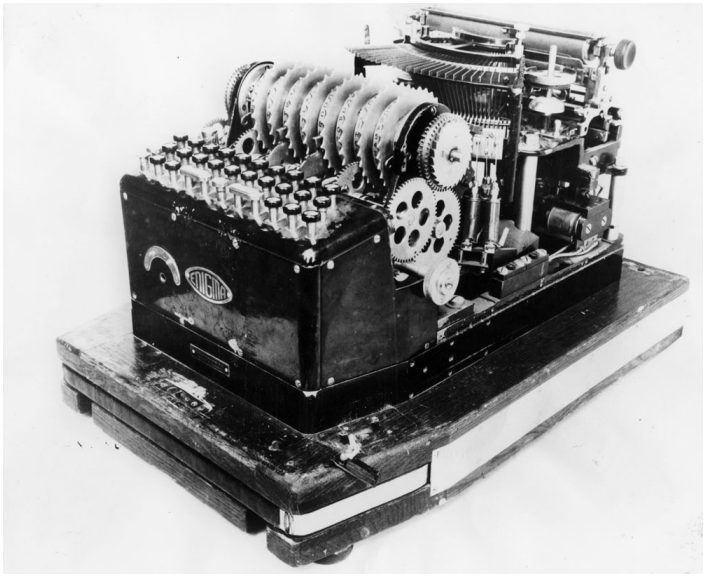

Figura 2. Máquina Enigma. Alemania, Segunda Guerra Mundial.

La siguiente gran revolución aparece a finales de los años sesenta, con el desarrollo de la criptografía de clave pública. Hasta entonces, todas las transformaciones eran simétricas, en el sentido que las partes debían intercambiar una misma clave con la cual se cifrara y descifrara la información. Posteriormente, surgió la criptografía asimétrica o de clave pública, en la cual se usan dos claves, una de ellas, como su nombre lo dice, es conocida por el público o aquellos receptores con quienes se quiera preservar un servicio de seguridad, y la otra, llamada privada, es solamente conocida por el dueño del par de claves pública y privada (Menezes *et al.*, 1997).

Figura 3. Criptografía simétrica y asimétrica.

En plena estandarización de los algoritmos pertenecientes a la criptografía moderna, por parte del Instituto Nacional de Estándares y Tecnología (NIST, 2018a), en los años setenta, se tienen las primeras ideas relacionadas con la criptografía cuántica. Aunque es hasta los ochenta cuando se muestran las publicaciones iniciales de nuevos protocolos, los cuales basaban su seguridad en los principios de la mecánica cuántica, disciplina de la física encargada de brindar una descripción fundamental de la naturaleza a escalas espaciales pequeñas (Chen *et al.*, 2016). De ahí, que en los años noventa, los algoritmos criptográficos modernos empezaron a verse afectados por la computación cuántica, lo que, con el paso de los años, dio pie al diseño de algoritmos postcuánticos que a la fecha se encuentran concursando hacia la estandarización por el NIST.

Figura 4. Procesador cuántico de la compañía Google.

La criptografía postcuántica en sus inicios

En los años noventa el profesor de matemáticas aplicadas del MIT Peter Shor propuso un algoritmo que descompone un número entero en sus factores primos (Shor, 1994). Al contar con un ordenador con recurso ilimitado, que no trabaje a nivel de voltajes eléctricos sino con partículas que puedan tener dos estados al mismo tiempo, dicho algoritmo podría utilizarse para "romper" algoritmos modernos de clave asimétrica. De hecho, a la fecha, el algoritmo de Shor y el algoritmo de Grover, correspondientes al cómputo cuántico, han podido comprometer algunos de los algoritmos utilizados desde la criptografía moderna hasta estos días.

La existencia de este tipo de algoritmos ha provocado dudas relacionadas con el uso de los algoritmos criptográficos modernos, ya que su seguridad quedaría expuesta y como consecuencia, también la de aquellas soluciones que los utilicen (Bernstein, 2009). De ahí, que la comunidad científica ha invertido mucho tiempo en el diseño de nuevos algoritmos criptográficos resistentes a ataques efectuados con computadoras cuánticas, conocidos como algoritmos postcuánticos. Este diseño se ha hecho tomando en cuenta algunas consideraciones, entre las que destacan que el cómputo cuántico usa reglas que son poco intuitivas, y que algunos cálculos se pueden realizar

exponencialmente más rápido que con el cómputo clásico. Es decir, cuando los algoritmos de la criptografía moderna empezaron a ser comprometidos por el cómputo cuántico, surgió la criptografía postcuántica, que hace referencia a los algoritmos diseñados para resistir ataques de computadoras cuánticas.

Estandarización de algoritmos postcuánticos

Algunos cuerpos de estandarización han reconocido la urgencia de cambiar y utilizar algoritmos que sean seguros ante ataques de computadoras cuánticas, lo que cobra importancia dado que muchas aplicaciones criptográficas requieren que todas las entidades participantes utilicen el mismo algoritmo. De ahí que la estandarización de algoritmos se observa como un prerrequisito para el amplio uso de los mismos. De hecho, algunos estándares *de facto* son tomados por distintos cuerpos de estandarización, aun cuando los procesos formales de estandarización son ampliamente vistos como una forma de reducir riesgos.

Por ejemplo, el grupo de trabajo de ingeniería en internet (Internet Engineering Task Force [IETF], 2018) y su rama de investigación Internet Research Task Force (IRTF) se encuentran como líderes terminando la estandarización de algoritmos de firma basados en *hash* (o resumen, ya que, a partir de una entrada de longitud variable, obtienen una salida de longitud constante). Algunas otras organizaciones que están interesadas en la estandarización de la criptografía postcuántica son la European Telecommunications Standards Institute (ETSI, Dahmen-Lhuissier, 2015), con su grupo de trabajo llamado Quantum-safe, así como ISO (2018) y OASIS (2018). Adicionalmente, en agosto de 2015, la Agencia de Seguridad Nacional (NSA, por sus siglas en inglés) anunció que prefería que los socios y proveedores invirtieran pronto en una transición hacia la criptografía postcuántica, en lugar de otro tipo de criptografía moderna. Recomendaron que aquellos que aún no hayan realizado la transición a la criptografía moderna, opten por prepararse para una transición a los algoritmos resistentes a ataques efectuados por computadoras cuánticas.

En 2015, debido a la preocupación latente de que una computadora cuántica puede romper los algoritmos criptográficos actuales, el NIST comenzó una investigación sobre algoritmos criptográficos asimétricos y firmas digitales que no sean susceptibles a ataques mediante algoritmos cuánticos.

Desde aquel entonces, el NIST llevó a cabo un taller para involucrar a los académicos interesados, de la industria y del gobierno, el cual llamó *Taller de Post Quantum* y se llevó a cabo del 2 al 3 de abril de 2015 (Workshop on Cybersecurity in a Post-Quantum World, 2015). En este taller, el NIST buscó discutir temas relacionados con la criptografía postcuántica y su potencial estandarización futura. De ahí, que, en el año 2017, el NIST empezó un proceso de solicitud, evaluación y estandarización de uno o más algoritmos asimétricos, resistentes a ataques cuánticos. Este proceso será de múltiples rondas de evaluación y durará aproximadamente de tres a cinco años (NIST, 2018c).

La idea principal en este proceso es que los nuevos estándares para criptografía asimétrica especifiquen uno o más algoritmos de cifrado para todo el mundo, para que, de esta manera sean capaces de proteger toda la información aún después de la amenaza fija de computadoras cuánticas. De esta manera, en abril de 2018, los algoritmos aceptados en la primera ronda de evaluación fueron invitados a discutir públicamente su propuesta en la conferencia PQCrypto2018.

Cabe destacar que en la primera ronda de evaluación se recibieron alrededor de 70 propuestas, las cuales tuvieron que cumplir con los requisitos mínimos de aceptabilidad, presentación y de evaluación para los algoritmos candidatos. De los candidatos recibidos en esta ronda de evaluación, al menos cinco fueron descartados. Posteriormente, en enero del 2019, se publicó la lista de los 26 algoritmos que pasan a nuevas evaluaciones, de los que se espera que los resultados estén antes que termine el año.

Con base en todo esto, el trabajo que está realizando el NIST está siendo tomado como referencia por las distintas organizaciones, para hacer la migración de algoritmos modernos hacia algoritmos criptográficos postcuánticos.

Niveles de seguridad aplicables a los algoritmos postcuánticos

En 2001 el NIST emitió el Estándar Federales de Procesamiento de la Información 140-2 (FIPS, del inglés Federal Information Processing Standards). Éste se enfoca en detallar la acreditación de módulos criptográficos desde el punto de vista de componentes de *software* y de *hardware* (NIST, 2001). Dicho estándar considera, entre otras cosas, los cuatro niveles de seguridad a los que se deben ajustar todos los módulos criptográficos, que son los niveles en los que basan su seguridad aquellos algoritmos postcuánticos que están siendo evaluados para su estandarización:

- Nivel 1. El nivel más bajo de seguridad, no especifica un mecanismo de seguridad físico, pero sí impone requisitos de seguridad básicos. Es utilizado para componentes de *software* y *firmware* de un módulo criptográfico.
- Nivel 2. Requiere, como mínimo, la autenticación basada en roles, en la que un módulo criptográfico autentifica la autorización de un operador basado en el cargo del usuario.
- Nivel 3. Se añade una resistencia a la intrusión física. Asimismo, incluye protección criptográfica eficaz y administración de clave, además de la autenticación basada en identidad y separación física o lógica.
- Nivel 4. El máximo nivel de seguridad. Incluye protección avanzada contra intrusos, además de que puede funcionar en entornos que no estén protegidos físicamente.

Además, en el 2017, el NIST describió los niveles de seguridad cuatro y cinco como "excesivas demostrables". Los niveles dos y tres como "seguras-demostrables para

un futuro previsible" y el primer nivel de seguridad como "seguras-demostrables para un futuro previsible, a menos que las computadoras cuánticas mejoren en un tiempo más rápido de lo que se anticipan".

Áreas de oportunidad detectadas

Una de las preocupaciones principales que manifiesta la comunidad científica y el NIST es el uso de diferentes algoritmos postcuánticos, dentro de la industria y las diferentes organizaciones. De ahí que sus retos y áreas de oportunidad detectadas se pueden centrar en lo siguiente:

- Tamaño de claves. En muchos de los casos, los algoritmos hacen uso de claves muy grandes, lo que genera que la velocidad de procesamiento se vea afectada significativamente.
- Tamaño de firma. Dependiendo del tipo de algoritmo, en algunos de ellos, el tamaño de la firma es importante, puesto que es directamente proporcional al tamaño de la longitud de la clave, por lo que se afecta la velocidad de la firma.
- Velocidad en cifrado, firma y verificación. Existe una relación entre la velocidad y los tamaños de firmas y de clave, puesto que mientras más grande sean estos, la velocidad disminuye.
- Flexibilidad y adaptación entre distintos algoritmos. El proceso de estandarización no especifica que los algoritmos deben trabajar solos, es decir, que no pueden trabajar en conjunto con algún otro algoritmo. Algunos de los algoritmos postcuánticos son capaces de trabajar mano a mano con otros, por lo que generan mayor protección, lo que les da ventaja sobre los demás competidores.
- Utilizar como base algoritmos cuya resistencia esté comprobada ante ataques cuánticos. Existen algunos algoritmos que se creen seguros ante ataques de computadoras cuánticas, pero la mayoría de los algoritmos recibidos por el NIST no hacen uso de ellos, por lo tanto, su resistencia ante los ataques cuánticos no está comprobada.
- Capacidad de memoria. Estos algoritmos tienen la ventaja de utilizar un espacio reducido de memoria, el cual se reduciría aún más si se reduce la longitud de la clave y como consecuencia el tamaño de la firma.
- Facilidad de implementación. Los algoritmos postcuánticos deben poder ser implementados de una manera sencilla en cualquier tipo de sistema dentro de la industria que así lo requiera, entre los que se destacan sistemas embebidos con muy pocos bits o computadoras clásicas.

Conclusión

No se tiene una fecha exacta para la llegada de las computadoras cuánticas, pero no se debe esperar hasta su llegada, sino que es importante estar preparados para el uso de algoritmos potscuánticos en los dispositivos móviles de uso cotidiano.

El desempeño de algoritmos postcuánticos dentro de dispositivos con características diversas se deja ver como una gran preocupación. Esto debido a la longitud de llave que ellos poseen, y a que aún no se sabe cómo se comportarán en dispositivos con poder de cómputo limitado. De ahí que el diseño de rutinas eficientes podría incrementar la velocidad de procesamiento, inclusive, dentro de la generación de claves criptográficas.

De hecho, el comportamiento de los algoritmos postcuánticos dentro de dispositivos con recursos limitados, entre los que destacan memoria y energía, requiere ser observado con detalle dado que las operaciones matemáticas que deben ejecutar podrían generar que el dispositivo no responda eficazmente dentro de su escenario de aplicación correspondiente.

La revisión y análisis de las diferentes implementaciones de los algoritmos postcuánticos que se encuentran disponibles en internet permitirá determinar con exactitud, en qué parte del código existen áreas de oportunidad, con lo cual se puede desvincular la relación existente entre la velocidad y los tamaños de las claves criptográficas.

Agradecimientos

Los autores agradecen al Instituto Politécnico Nacional por el apoyo otorgado para la realización de este trabajo, a través de los proyectos SIP 1917 y 20196694.

Referencias

- Bernstein, D. J. (2009). Introduction to post-quantum cryptography. En *Post-quantum cryptography* (pp. 1-14). Berlin, Heidelberg: Springer.
- Chen, L., Jordan, S., Liu, Y. K., Moody, D., Peralta, R. y Smith-Tone, D. (2016). *Report on post-quantum cryptography*. Gaithersburg, MD: US Department of Commerce, National Institute of Standards and Technology. DOI: http://dx.doi.org/10.6028/NIST.IR.8105.
- Dahmen-Lhuissier, S. (2015). Quantum-Safe Cryptography (QSC). Recuperado de: https://www.etsi.org/newsroom/news/11-technologies-clusters/technologies?start=20.
- Hallgren, S. y Vollmer, U. (2009). Quantum computing. En *Post-quantum cryptography* (pp. 15-34). Berlin, Heidelberg: Springer.
- Iashchenko, V. V. (2002). *Cryptography: An Introduction*. s.l.: American Mathematical Society.
- Internet Engineering Task Force (IETF). (2018). Recuperado de: https://www.ietf.org/.

- ISO (2018). *International Organization for Standardization.* Recuperado de: https://www.iso.org/home.html.
- Menezes, A., van Oorschot, P., Vanstone, S. y Rosen, K. (1997). *Handbook of Applied Cryptography.* Boca Raton: CRC Press.
- National Institute of Standards and Technology (NIST) (2001). FIPS *140-2: Security Requirements for Cryptographic Modules.* Recuperado de: https://csrc.nist.gov/publications/detail/fips/140/2/final.
- National Institute of Standards and Technology (NIST). (2018a). *National Institute of Standards and Technology.* Recuperado de https://www.nist.gov/.
- National Institute of Standards and Technology (NIST). (2018b). Post-Quantum Cryptography. Recuperado de: https://csrc.nist.gov/Projects/Post-Quantum-Cryptography.
- National Institute of Standards and Technology (NIST). (2018c). Post-Quantum Cryptography Standardization. Recuperado de: https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantumcryptography standardization.
- Advancing open standards for the information society (OASIS). 2018). *Organization of Advancing Open Standards for the Information Society.* Recuperado de: https://www.oasis-open.org/.
- Shor, P. W. (1994). Algorithms for quantum computation: Discrete logarithms and factoring. En *Proceedings. 35th Annual Symposium on Foundations of Computer Science* (pp. 124-134). DOI: https://doi.org/10.1109/SFCS.1994.365700.
- Singh, S. (2000). *The code book.* Nueva York, NY: Anchor Books.
- Workshop on Cybersecurity in a Post-Quantum World. (2015) Recuperado de: https://csrc.nist.gov/Events/2015/Workshop-on-Cybersecurity-in-a-Post-Quantum-World.
- Solana, P. X (2009). *Antecedentes y perspectivas de estudio en historia de la Criptografía* [tesis de licenciatura]. Recuperado de: https://e-archivo.uc3m.es/handle/10016/6173.

Cómo citar este artículo

- Delgado Vargas, Kevin Andrae, De Abiega L'Eglisse, Alfonso Francisco, Gallegos-Garcia, Gina y Cabarcas, Daniel (2019). Un acercamiento a la línea del tiempo de los algoritmos criptográficos. *Revista Digital Universitaria* (RDU). Vol. 20, núm. 5 septiembre-octubre. DOI: http://doi.org/10.22201/codeic.16076079e.2019.v20n5.a7.

Recepción: 25/02/2019. Aprobación: 27/07/2019