Criptografía ligera

Martin Borgo, Isaías Reniero, Leandro Molina

Universidad Nacional de Entre Ríos

Facultad de Ciencias de la Administración

Licenciatura en Sistemas

martinborgo8@gmail.com, isa.reniero001@hotmail.com, LeandroRodrigoMolina@gmail.com

Abstract. La criptografía ligera (Lightweight Cryptography), es una rama de la criptografía que se enfoca en desarrollar algoritmos eficientes y de bajo consumo para su implementación en sistemas con recursos limitados, como sistemas embebidos, dispositivos IoT (Internet de las cosas) y microcontroladores. La ausencia de medidas de seguridad adecuadas en tales sistemas generan preocupaciones, especialmente cuando se trata de gestionar información sensible, en este contexto la criptografía ligera ofrece soluciones que permiten proteger eficazmente los datos y las comunicaciones, sin sacrificar la eficiencia de los recursos. En este artículo se realiza una recopilación de todos los conceptos, avances y tendencias que se fueron dando a lo largo de los años en este campo de la criptografía.

Keywords: Criptografía ligera, Block ciphers, IoT, Seguridad.

1 Introducción

La criptografía ligera (rama de la criptografía) es uno de los temas de la actualidad que se encuentra en auge. Es usada en dispositivos donde su poder de cómputo es reducido, a estos dispositivos actualmente se les conoce como IoT (Internet of Things o Internet de las Cosas), aunque en sus inicio recibía el nombre de red de sensores. Muchos de estos dispositivos utilizan microcontroladores de muy bajo consumo que solo pueden permitirse una pequeña parte de su cómputo a la seguridad[1]. Esto provoca que los algoritmos clásicos de criptografía (Como los basados en AES Advanced Encryption Standard) no puedan ser usados, debido a la alta latencia y consumo de energía que presentaron en estos dispositivos. La criptografía ligera nos brinda una gran variedad de algoritmos "livianos" que han sido diseñados para garantizar confidencialidad, autenticidad e integridad de los datos en los dispositivos IoT. Son algoritmos desarrollados por los ámbitos académicos, agencias estatales o propietarios. En sus inicios, el sector que más utilizaba esto era el industrial:

> 'Un ejemplo común de este uso es el de las redes de sensores. Estas redes tienen como objetivo conectar grandes cantidades de sensores muy simples a un centro principal. Estos sensores funcionan con baterías y/o generarían su propia energía utilizando, por ejemplo, paneles solares. Los algoritmos criptográficos deben usarse en los canales de comunicación entre los sensores y su centro para proporcionar seguridad, autenticidad e integridad de los mensajes. Sin embargo, debido a la muy baja energía disponible y porque la seguridad es un gasto adicional a la funcionalidad real del dispositivo, los algoritmos criptográficos deben ser lo más 'pequeños' posible.' (Biryukov & Perrin, 2017, p. 1)

2 Desarrollo de Trabajo

2.1 Estandarización de la Criptografía Ligera: ISO/IEC 18033 y 29192

2.2 Clasificación y Consideraciones en el Diseño

2.3 Algoritmos Criptográficos Ligeros: Tendencias y Desafíos

3 Resultados Obtenidos y Esperados

4 Conclusión

5 Referencias

Biryukov, A., & Perrin, L. (2017). State of the art in lightweight symmetric cryptography. *Cryptology ePrint Archive*.

Cipriano, M. J. (2021). *Criptografía liviana e Internet de las Cosas: Confidencialidad de la información mediante Stream Ciphers estandarizados en las normas ISO/IEC 18033 y 29192* [Tesis doctoral, Universidad Nacional de La Plata].

[1]Es importante tener en cuenta que, aunque la criptografía ligera es útil para dispositivos con recursos limitados, los avances en la tecnología a menudo influyen en lo que se considera "ligero". Lo que se considera ligero en un momento dado podría no serlo en un futuro, a medida que la capacidad de los dispositivos mejore.

Eterovic, J., Cipriano, M., García, E., & Torres, L. M. (2019). Criptografía Ligera en Internet de las Cosas para la Industria. *XXV Congreso Argentino de Ciencias de la Computación (CACIC)(Universidad Nacional de Río Cuarto, Córdoba, 14 al 18 de octubre de 2019)*.

Eterovic, J. E., & Cipriano, M. J. (2018). Stream Ciphers livianos estandarizados mediante normas internacionales para ser usados en Internet de las Cosas. *Sistemas, Cibernética e Informática*, *15*(2-2018).

Tilborg, H. C. v., & Jajodia, S. (s.f.). Encyclopedia of Cryptography and Security, 2011.

Wehbe, R., Armas, A. d., & Barrera, E. (2022). Criptografía liviana para objetos conectados. *XXIV Workshop de Investigadores en Ciencias de la Computación (WICC 2022, Mendoza)*.