# Métodos de Criptografía Ligera para brindar Servicios de Seguridad al Internet de las Cosas

Carlos Andres Lara-Nino
carlos.lara@cinvestav.mx
CINVESTAV Tamaulipas
Ciudad Victoria, Tamaulipas, México

Arturo Diaz-Perez
adiaz@cs.cinvestav.mx
CINVESTAV Guadalajara
Zapopan, Jalisco, México

Miguel Morales-Sandoval
mmorales@tamps.cinvestav.mx
CINVESTAV Tamaulipas
Ciudad Victoria, Tamaulipas, México

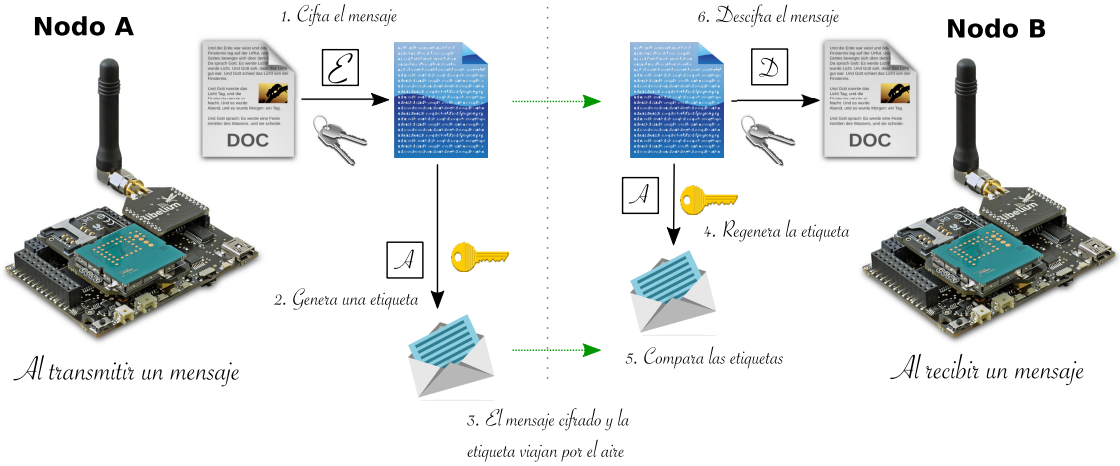


**Figura 1: Establecimiento de un canal de comunicación seguro entre dos dispositivos inalámbricos.** Los mensajes transmitidos entre dos dispositivos inalámbricos deben ser protegidos mediante técnicas de seguridad de la información. Si no hay seguridad un atacante podría conocer el contenido de los mensajes o modificarlos. En el esquema de seguridad ilustrado se hace evidente la necesidad de contar con algoritmos de *llave pública* y de *llave simétrica*: mientras que unos consiguen que los dispositivos obtengan secretos compartidos, otros aseguran grandes volúmenes de datos.

## RESUMEN

El *Internet de las Cosas* (IoT)[1] es una tecnología emergente que promete revolucionar la forma en la que interactuamos con el mundo. Bajo este paradigma, objetos cotidianos son dotados con capacidades de sensado, procesamiento de datos, y conexión a internet, lo que permite tener acceso remoto y en tiempo real a la información de la que disponen. Por ejemplo, la temperatura de nuestro hogar, los contenidos del refrigerador, el nivel de combustible de nuestro auto, entre muchos otros. En algunos casos esta información puede ser sensible en si misma; en otros, el amplio volumen de los datos puede dar pistas sobre el comportamiento de los usuarios, generando posibles riesgos de privacidad y seguridad. En ambos escenarios es evidente la necesidad de proteger los datos. El principal reto para ello se encuentra en las restricciones mismas de los nodos de IoT: tienen bajo poder de cómputo, ocasionalmente se alimentan por baterías, disponen de poco almacenamiento, y su ancho de banda es limitado. La *Criptografía Ligera* busca con métodos novedosos proporcionar *servicios de seguridad* adecuados para estos sistemas restringidos, de modo que se pueda garantizar la *seguridad de la información* en el IoT.

[1]IoT, del inglés *Internet of Things*.

## PALABRAS CLAVE

internet de las cosas, criptografía, criptografía ligera, seguridad en hardware

**Citar como:**
Carlos Andres Lara-Nino, Arturo Diaz-Perez, and Miguel Morales-Sandoval. 2019. Métodos de Criptografía Ligera para brindar Servicios de Seguridad al Internet de las Cosas. En *Memorias del Octavo Encuentro de Estudiantes Destacados en el área de Tecnologías de la Información*. CINVESTAV, Ciudad Victoria, TAMPS, MEX, 4 páginas.

## SEGURIDAD PARA EL IOT

En la actualidad, la modernización y automatización de diversas tareas cotidianas ha impulsado el desarrollo de nuevas tecnologías. Uno de los esquemas emergentes más prometedores es conocido como el IoT [1]. Bajo este paradigma, objetos cotidianos como autos, edificios, y electrodomésticos son dotados con acceso a internet y capacidades para cuantificar magnitudes en su entorno. Esto con el objetivo de que el usuario final pueda consultar la información

recolectada por los dispositivos a través del internet. La premisa de utilidad de esta tecnología reside en que, al contar con más información, el usuario puede tomar mejores decisiones.

## El Internet de las Cosas

Las principales características de IoT son tres:

- Se componen de dispositivos físicamente pequeños, los cuales suelen ser inalámbricos.
- Es una colección de redes heterogéneas de alta densidad con topología variable.
- Se considera una tecnología ubicua, por lo cual los dispositivos que conforman las redes pueden desplegarse en ambientes no controlados.

Los dispositivos de IoT son físicamente pequeños para conseguir bajos costos de producción. Esto genera que la capacidad de las unidades de procesamiento empleadas, así como la memoria disponible sean limitadas. En aplicaciones particulares del IoT, como las Redes Inalámbricas de Sensores[2] (Figura 2), incluso es necesario que los dispositivos se alimenten por baterías. Por el costo monetario, estas baterías también suelen ser pequeñas. En estos casos se considera que la red operará mientras que tenga energía, por ende, el tiempo de vida estará limitado por el consumo de energía de los dispositivos.

IoT es una tecnología relativamente nueva, habiéndose popularizado en los últimos diez años. Se estima que su crecimiento continuará al grado de contar con billones de dispositivos en el futuro cercano [2]. Este rápido desarrollo ha traído consigo la modernización de distintos sectores de la sociedad: seguridad, comercio, construcción, manufactura, salud, entre otros. No obstante, también ha impulsado la proliferación de riesgos de seguridad para los usuarios [3]. Como se ha mencionado, los dispositivos de IoT operan con información obtenida del medio. Dada la aplicación, esta información puede ser inherentemente sensible; o por su volumen esta información puede ser usada para inferir comportamientos del usuario [4].

## Riesgos de seguridad

Un actor malicioso o atacante puede buscar hacer uso no autorizado de los datos con los que operan las redes de IoT. Si consigue acceso no autorizado a la información se dice que se vulnera la *confidencialidad* de la misma. Si el atacante altera los datos, entonces se compromete su *integridad* o *autenticidad*. En algunos casos el objetivo puede ser irrumpir el flujo de información de manera que el usuario legítimo no pueda tener acceso al servicio o que la calidad de éste baje. Estos son algunos de los riesgos de seguridad más habituales a los que se enfrentan los entornos de red como lo es el IoT. Estos riesgos se pueden materializar en ataques mediante distintas técnicas. Además, existe una amplia gama de amenazas que crece conforme las estrategias de ataque se vuelven más sofisticadas [3].

Para mitigar los riesgos antes mencionados es necesario proporcionar a los dispositivos de IoT con servicios de seguridad. Estos servicios reciben el nombre de los preceptos que tratan de hacer cumplir: confidencialidad, integridad, autenticidad, disponibilidad.

[2]WSN, del inglés *Wireless Sensor Networks*.

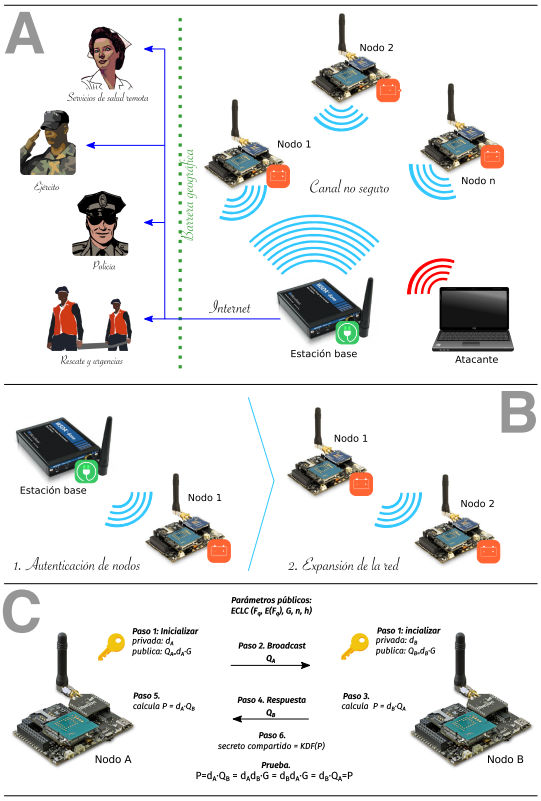


**Figura 2: Ecosistema de WSN y su seguridad. A)** Los elementos básicos de estas redes son la *estación base* y los nodos o *motes*; estos se comunican a través del aire donde un atacante puede escuchar el canal. La estación base sirve como punto de acceso al internet. **B)** En la formación de estas redes la topología no es conocida, por lo que cada dispositivo debe ser capaz de establecer un canal seguro con cualquier otro elemento en la red. **C)** Los métodos criptográficos emplean *protocols* para ofrecer distintos servicios de seguridad; las operaciones criptográficas mostradas en la Figura 1 requieren secretos compartidos, estos se obtienen mediante esquemas de establecimiento de llaves como el ilustrado.

Existen otros servicios de seguridad, pero los citados se consideran como los más relevantes en la literatura [5].

## Criptografía y seguridad de la información

En el área de la *criptografía* existen herramientas o algoritmos ampliamente estudiados que permiten proporcionar distintos servicios de seguridad. Los *cifradores* se usan para brindar confidencialidad al enmascarar los datos—la Figura 3 ilustra la operación de una de estas herramientas. Los *códigos de autenticidad* de mensajes pueden usarse, como su nombre lo indica, para garantizar la integridad y autenticidad de los mensajes en el IoT. La autenticidad de dispositivos es útil para implementar políticas de acceso a la red y mitigar ataques contra la disponibilidad de servicio. Esto último se consigue empleando protocolos de intercambio de información. Estas herramientas han sido estandarizadas a lo largo de los años en distintas normativas que permiten la interoperabilidad entre

aplicaciones distintas. Desafortunadamente, en la mayoría de los casos las herramientas criptográficas estandarizadas no consideran las restricciones del dispositivo donde se implementarán.

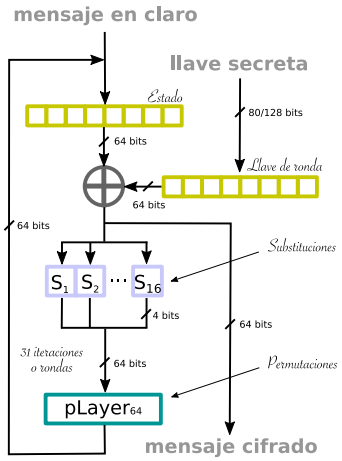


**Figura 3: Operación del algoritmo de cifrado** PRESENT. Este cifrador *ligero* opera sobre bloques de 64-bits del mensaje aplicando substituciones y permutaciones a los datos a lo largo de 31 rondas. Los valores intermedios se almacenan en una memoria o "estado."

El costo que se genera del uso de soluciones de seguridad basadas en criptografía es alto; éste se puede medir a través del *uso de memoria*, el *tiempo de procesamiento*, el *gasto de ancho de banda*, y el *consumo de energía*. Al mismo tiempo, las soluciones criptográficas son deseables pues garantizan cierto nivel de seguridad y auditoría. En sistemas de información convencionales, cubrir los costos asociados con seguridad se consideran un compromiso aceptable. Sin embargo, para aplicaciones como el IoT, el sobre costo que surge al proporcionar al dispositivo con servicios de seguridad puede limitar el uso de este tipo de algoritmos. Es necesario conseguir soluciones de seguridad criptográficas adecuadas para las restricciones de la aplicación [6]. Tales propuestas han sido denominadas *ligeras* en la literatura.

## ¿Criptografía ligera?

Aun cuando no existe una definición precisa en el estado del arte sobre lo que representa un algoritmo "ligero", este término se usa para referirse a diseños arquitecturales simplificados que reducen el número de operaciones realizadas con un impacto moderado en la seguridad del algoritmo. La reducción en el consumo de energía impactará directamente en el tiempo de vida del dispositivo, mientras que la reducción del área física se traducirá en menores costos de producción.

En nuestra propuesta, por criptografía ligera definimos a *la rama de la criptografía que estudia el uso de algoritmos criptográficos adaptados a los requerimientos de aplicaciones que cuentan con recursos limitados en materia de: capacidad de procesamiento, hardware disponible, memoria, energía, canal de comunicaciones, entre otros.* Algunos ejemplos de tales aplicaciones son los nodos de IoT, las tarjetas de identificación por radio frecuencia, y los nodos de las redes de sensores.

## Retos para la seguridad

IEEE 802.15.4 es uno de los principales estándares que rigen la operación de aplicaciones restringidas. En esta norma se definen mecanismos de seguridad para cubrir los servicios de confidencialidad, integridad, autenticidad y disponibilidad. No obstante, los algoritmos especificados dependen de la existencia de piezas de información compartidas entre los dispositivos que desean comunicarse: las llaves criptográficas. Algoritmos como los cifradores y las funciones para generar códigos de autenticidad de mensaje emplean llaves criptográficas. La seguridad del sistema depende de que esta pieza de información permanezca secreta. En IEEE 802.15.4 se asume que los dispositivos cuentan con estos secretos compartidos, pero no se especifica el cómo obtenerlos. Se puede suponer que se deben usar mecanismos de establecimiento de llaves estandarizados, pero esto implica incurrir en costos altos para las aplicaciones restringidas.

El establecimiento de llaves es un proceso o protocolo mediante el cual un secreto compartido se hace disponible para dos o más participantes, para su subsecuente uso criptográfico. Este tipo de algoritmos puede dividirse en transporte de llaves y acuerdo de llaves. En el mecanismo o protocolo de transporte de llaves un participante crea o de alguna forma obtiene un valor secreto, y de forma segura lo transfiere a otro(s). En el mecanismo o protocolo de acuerdo de llaves un secreto compartido es generado por dos (o más) participantes, como función de la información contribuida por, o asociada con, cada uno de éstos, (idealmente) de forma que ningún participante pueda anticipar el valor resultante. Diseñar sistemas para la distribución, compartición o establecimiento de secretos que tengan un tamaño de implementación reducido y bajo consumo de energía es un problema abierto [7].

Los algoritmos de seguridad se pueden clasificar en dos grandes grupos de acuerdo al tipo de llaves utilizadas: cifradores y demás funciones que emplean una única llave para aplicar transformaciones directas sobre los datos, y que usan la misma llave en las respectivas transformaciones inversas se les llama *simétricos*; cuando estas llaves difieren se dice que existe un par de llaves y el algoritmo es *asimétrico*. En este par de llaves las piezas de información mantienen una relación, a una de las llaves se le llama secreta y es usada para generar la otra, coloquialmente conocida como *pública*. De este último nombre es que a la criptografía asimétrica se le llama "pública." El grueso de la criptografía utilizada actualmente se basa en construcciones simétricas dada su eficiencia. Sin embargo, algunas aplicaciones particulares resultan más sencillas en esquemas de llave pública, entre ellas el establecimiento de secretos compartidos.

Entre los sistemas asimétricos más ampliamente conocidos destacan el criptosistema RSA y los sistemas basados en curvas elípticas. En los últimos años, la Criptografía de Curva Elíptica[3] ha sido la mejor opción en cuanto a seguridad y eficiencia en materia de criptografía de llave pública. Esta ha servido como fundamento para la mayoría de los sistemas de establecimiento de llaves estandarizados, usados extensivamente en diversos tipos de aplicaciones. A pesar de la eficiencia de ECC, los dispositivos que implementan este tipo de soluciones deben resolver operaciones costosas. La más importante de ellas es conocida como multiplicación escalar—la Figura

[3] ECC, del inglés *Elliptic Curve Cryptography*.

4 presenta una arquitectura hardware diseñada para resolver este procedimiento.

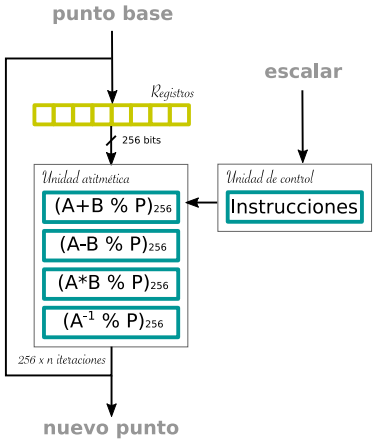


**Figura 4: Esquema de procesamiento para resolver una multiplicación escalar.** El punto base se *suma* con si mismo $k-1$ veces, donde $k$ es conocido como escalar. Estas *sumas* son operaciones de curva que se componen por operaciones de campo (modulares). El número de iteraciones es $\log_2 k$, multiplicado por el número de operaciones de campo requeridas ($n$) en cada *suma* de punto. La complejidad de estos sistemas radica en la dificultad de computar las operaciones modulares y el gran número de iteraciones.

Optimizar el procesamiento de la multiplicación escalar es una estrategia común para obtener soluciones eficientes basadas en ECC. Para implementaciones en software, los principales objetivos de diseño suelen ser reducir el número de ciclos de procesamiento y el uso de memoria requeridos por multiplicación escalar. El uso de soluciones basadas en hardware representa una alternativa para reducir la carga de trabajo del procesador. Esto se consigue mediante el uso de aceleradores o coprocesadores para tareas criptográficas. En la concepción de estos módulos, los objetivos de diseño se orientan a minimizar el área de implementación y el consumo de energía.

En este proyecto se propone el estudio del uso de algoritmos criptográficos ligeros en ambientes de aplicación propios del ecosistema de IoT. Se hace particular énfasis en la necesidad de investigar estrategias adecuadas para el diseño e implementación de soluciones de establecimiento de llaves.

## ¿Cómo se crean estas soluciones?

Las implementaciones de sistemas de seguridad en hardware resultan atractivas para dispositivos con limitado poder de procesamiento ya que es sencillo introducir aceleradores de cómputo en sistemas legado. Mientras que una solución en software puede no requerir modificaciones a la plataforma física del dispositivo, los procesadores equipados en estos sistemas pueden no ser aptos para ejecutar las complejas operaciones criptográficas.

Un coprocesador dedicado para tareas de seguridad puede ser equipado como un circuito integrado de aplicación específica[4] o un

[4] ASIC, del inglés *Application Scpecific Integrated Circuit.*

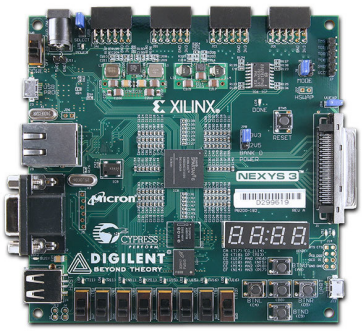


**Figura 5: La tarjeta de prototipado Nexys 3 equipada con un FPGA Spartan-6 de la compañía Xilinx.**

núcleo reconfigurable basado en arreglos de compuertas programables de campo[5]—estos últimos ilustrados en la Figura 5. Estos elementos pueden desarrollar tareas particulares, diseñados con objetivos específicos en cuanto al nivel de seguridad, la tasa de procesamiento, el tamaño de implementación y el consumo de energía.

Tradicionalmente se ha considerado que el uso de ASICs ofrece ventajas sobre FPGAs, particularmente con relación al desempeño y al consumo de energía, sin embargo, los avances en el diseño de FPGAs han reducido esta diferencia [8]. El uso de FPGAs resulta particularmente atractivo para aplicaciones de seguridad ya que la reconfigurabilidad puede ser utilizada para actualizar los protocolos o algoritmos en etapa de post producción en caso de que se detecte una vulnerabilidad. Aunado a esto, la producción de ASICs usualmente se desarrolla en ambientes no controlados por el diseñador del circuito y asume que el fabricante del dispositivo no ha alterado el diseño para inducir comportamientos no deseados en el producto final [9].

## REFERENCIAS

[1] A. Zanella, N. Bui, A. Castellani, L. Vangelista, and M. Zorzi, "Internet of Things for Smart Cities," *IEEE Internet of Things Journal*, vol. 1, pp. 22–32, Feb 2014.
[2] L. Columbus, "2018 Roundup Of Internet Of Things Forecasts And Market Estimates." [Online] www.forbes.com, 2018.
[3] Y. Yang, L. Wu, G. Yin, L. Li, and H. Zhao, "A Survey on Security and Privacy Issues in Internet-of-Things," *IEEE Internet of Things Journal*, vol. 4, pp. 1250–1258, Oct 2017.
[4] R. Perez-Torres, C. Torres-Huitzil, and H. Galeana-Zapien, "An On-Device Cognitive Dynamic Systems Inspired Sensing Framework for the IoT," *IEEE Communications Magazine*, vol. 56, pp. 154–161, Sep. 2018.
[5] A. J. Menezes, S. A. Vanstone, and P. C. V. Oorschot, *Handbook of Applied Cryptography*. Boca Raton, FL, USA: CRC Press, Inc., 1st ed., 1996.
[6] Haowen Chan and A. Perrig, "Security and privacy in sensor networks," *Computer*, vol. 36, pp. 103–105, Oct 2003.
[7] A. Kumar and A. Aggarwal, "Lightweight cryptographic primitives for mobile ad hoc networks," in *Recent Trends in Computer Networks and Distributed Systems Security* (S. M. Thampi, A. Y. Zomaya, T. Strufe, J. M. Alcaraz Calero, and T. Thomas, eds.), (Berlin, Heidelberg), pp. 240–251, Springer Berlin Heidelberg, 2012.
[8] T. Tuan, A. Rahman, S. Das, S. Trimberger, and S. Kao, "A 90-nm low-power fpga for battery-powered applications," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 26, pp. 296–300, Feb 2007.
[9] H. Salmani and M. Tehranipoor, *Digital Circuit Vulnerabilities to Hardware Trojans*, pp. 37–51. Cham: Springer International Publishing, 2017.

[5] FPGA, del inglés *Field Programmable Gate Array.*