Trabajo practico 2 investigación

Borgo Martin, Reniero Isaias, Molina Leandro

September 17, 2023

1. Realizar una revisión bibliográfica y elaborar un resumen, de no menos de 2 carillas, del estado actual del conocimiento sobre el tema elegido, es decir describir la situación actual del tema abordado, lo que se conoce y lo que no, lo escrito y lo no escrito, lo evidente y lo tácito.

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 (publicados en revistas), agencias estatales o propietarios. Cuyo campo de aplicación en sus inicios fue 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)

[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.

Fue tal la relevancia que estaban teniendo estos algoritmos que en 2011 se estandarizan gran parte de estos con la ISO/IEC 18033, que en sus diferentes incisos quedan descritos y especificados cada uno de los métodos de encriptación que estaban siendo utilizados a nivel industrial, académico y gubernamental hasta dia de hoy. Aunque el paso más grande se dio en 2012 con la salida de la ISO/IEC 29192-1:2012 donde se introduce por primera vez el término criptografía ligera, brindando definiciones y estableciendo una serie de requerimientos de seguridad, implementación y clasificación. De la mano de la estandarización vienen un conjunto de ventajas, que (J. E. Eterovic & Cipriano, s.f.) mencionan los siguientes beneficios:

1. La libre disponibilidad del algoritmo para su uso.
2. Se cuenta con una descripción detallada de las funciones que lo conforman, como así también del diseño en general.
3. Se puede realizar una verificación del funcionamiento y conformidad mediante un grupo independiente de expertos.
4. La existencia de vectores de prueba[2] para corroborar del buen funcionamiento de los mismos.

Separándonos un poco del estándar, en (Wehbe et al., 2022) se dividen a los diferentes algoritmos de criptografía ligera en 4 grandes grupos:

- **Stream ciphers (cifrados de flujo)**: Es un cifrado simétrico que opera con una transformación que varía con el tiempo en dígitos individuales de texto plano. Una secuencia de texto plano se cifra usando una secuencia pseudoaleatoria, generada a partir de una clave secreta y un parámetro público. Cada dígito cifrado se obtiene combinando el dígito correspondiente de texto plano con esta secuencia.
- **Block ciphers (cifrados de bloque)**: Es un sistema que, para una clave específica k, define un algoritmo de cifrado que convierte un bloque de texto plano de n bits en un bloque de texto cifrado de n bits, y un algoritmo de descifrado correspondiente.
- **Funciones de hashing criptográficas**: Toman cadenas de entrada de longitud arbitraria y las convierten en cadenas de salida de longitud fija y corta, que es única (en teoría) para cada entrada única.
- **Algoritmos de criptografía asimétrica (Sistemas de clave pública, como RSA y curvas elípticas)**: Utiliza claves diferentes para cifrar y descifrar. Una clave puede ser pública, mientras que su contraparte debe mantenerse en secreto.

[2]Los vectores de pruebas son un conjunto de datos de entrada predefinidos y conocidos, utilizados para probar y verificar el correcto funcionamiento de un algoritmo.

Actualmente se proponen muchos algoritmos criptográficos donde sus diseños varían mucho, y cuya única similitud es la baja potencia requerida para su ejecución. La implementación o diseño de estos algoritmos están divididos en dos: hardware y software. Independientemente de eso, al momento de su diseño se debe hacer especial hincapié en el consumo de memoria, el tamaño de la implementación (código o circuitería requerida) y la velocidad o rendimiento del algoritmo. Lo que sí varía de un tipo de implementación a otra son los parámetros utilizados para indicar su eficiencia. Más allá de esos aspectos, no importa la implementación específica que se haga, ya que un algoritmo de criptografía ligera debe, idealmente, conseguir un equilibrio entre seguridad, rendimiento y costo.
A continuación mencionaremos los aspectos principales en los que se deben enfocar cada uno de los diseñadores e implementadores de acuerdo al tipo al tipo de implementación particular por la que se haya decantado. Si la implementación es por hardware para que este sea eficiente se deben tener en consideración los siguientes puntos:

- Debe minimizar el consumo de memoria, en RAM o el área de puerta en dispositivos con recursos limitados.
- El tamaño de la implementación debe ser optimizado, es decir, que el diseño debe ser lo más compacto posible para ocupar menos espacio en el chip.
- Debe considerar el acceso a la memoria no volátil y cómo se accede a las claves almacenadas en ella.
- Las operaciones como las permutaciones de bits, que son baratas en hardware, son las más preferidas.
- La estructura de la clave no debe requerir un estado de clave que se actualice en cada ronda, ya que esto sería costoso en términos de área de puerta.

Si la implementación es por software para que este sea eficiente se deberá considerar los siguientes puntos:

- Debe minimizar el consumo de memoria, en RAM utilizada.
- Las operaciones como las rotaciones de palabras, que son eficientes en software, pueden ser preferidas.
- Debe considerar la forma en que se accede a las claves y cómo se almacenan en la memoria.
- Las operaciones que son inherentemente costosas en software, como el manejo de bits a nivel individual, deben evitarse o minimizarse.
- Las estructuras de clave que pueden evaluarse "en el momento" (es decir, generadas en tiempo real durante la ejecución en lugar de pre-calculadas y almacenadas) son preferibles para mantener la eficiencia.

En (Biryukov & Perrin, 2017) enumeran en su artículo algunas de las tendencia que están siendo adoptando en el diseño de nuevos algoritmos criptográficos ligeros, donde se hace mención a las operaciones no lineales, operaciones lineales y se habla sobre el esquema de llaves.

Las operaciones no lineales son realmente necesarias en cualquier algoritmo de encriptación, ya que brindan una mayor protección contra ciertos ataques, concretamente los ataques de criptoanálisis[3] los ataques de fuerza bruta[4] y los ataques de canal lateral[5]. Dentro de los mecanismos utilizados en la criptografía ligera se encuentran las tabla de consultas(Look-up Table), las cuales son una estructura de datos que, suele ser implementada a través de cajas de sustitución[6](S-Boxes), estas se utilizan para realizar operaciones no lineales de manera más eficiente, y debido que pueden ser implementadas utilizando S-Boxes, permiten que los algoritmos que utilizan estas tablas puedan ser eficientemente implementados tanto por hardware como por software. Se menciona también a los algoritmos basados en segmentos de bits, que también hacen uso de S-Boxe de manera distinta que le permiten realizar operaciones bit a bit como AND y XOR, en palabras de w bits. Dado que esta tarea requiere un número limitado de operaciones lógicas, los algoritmos que utilizan este método se destacan por su eficiencia tanto en la implementación por software y hardware. Por último se encuentran los algoritmos basados en ARX (adición, rotación y XOR), que debido a su simplicidad, eficiencia y a la gran dispersión en los datos que se consigue con ellos, junto con el hecho de que la adición a nivel de software es extremadamente eficiente, hace que los algoritmos basados en ARX se encuentran entre los mejores en rendimiento para microcontroladores.

Las operaciones lineales, por otro lado, tienen un rol fundamental, ya que proveen de difusión a los datos. Entre los mecanismos mencionados por los autores se encuentran las matrices de dispersión máxima, las cuales proveen una dispersión adecuada de los datos, al mismo tiempo que minimiza el costo computacional, aumentando la protección contra criptoanálisis lineales y diferenciales. La permutación de bits también es otro mecanismo que está siendo altamente utilizado en ciertas plataformas, debido a que, en términos generales, su implementación por hardware se puede realizar a bajo costo, con el inconveniente que por el momento son un poco costosas de realizarse a nivel software, es por esa razón que son mayormente empleados por dispositivos RFID y similares. Por último nombran a los algoritmos que se basan en rotación y XOR (RX),

[3]El criptoanálisis se centra en estudiar y analizar los sistemas criptográficos para poder vulnerar su seguridad, algunas de las técnicas usadas en el reconocimiento de patrones de redundancia de los textos, el averiguar características del algoritmo de cifrado, entre otras.

[4]En los ataques de fuerza bruta se trata de descubrir la clave utilizada para cifrar la información, probando todas las combinaciones posibles, es un mecanismo útil cuando se sabe que las llaves de cifrado son cortas.

[5]Un ataque de canal lateral se centra en el análisis de la información indirecta que se filtra durante el proceso de cifrado o descifrado, con el objetivo de descubrir información sensible o claves de seguridad. Esta información puede ser la variación en el consumo eléctrico, el tiempo de respuesta del dispositivo, entre otros.

[6]Las S-Boxes son funciones booleanas vectoriales no lineales, que toman un número determinado de bits de entrada y los transforman en otro número de bits de salida, que no necesariamente tiene que ser la misma cantidad de bits.

estos brindan una difusión apropiada, siendo barato de implementar tanto por software como por hardware, acarreando casi todas las ventajas de los algoritmos ARX pero con incluso un costo un poco menor.
Los autores finalizan hablando del esquemas de llaves, que debido a su elevado consumo en términos de RAM, hace que los diseñadores opten por implementar estos algoritmos utilizando llaves de corta extensión, dejándolos expuestos a ataques de llaves relacionadas[7], si bien en la actualidad existen una serie de algoritmos que se jactan de ser inmunes a este tipo de ataques, esto lo consiguen añadiendo más rondas al momento de encriptar los datos o a través de esquemas de llaves más complejos, en ambos casos este tipo de alternativas no es muy preferida a la hora de crear este tipo de algoritmos.
Llegando al final del mismo artículo, se realiza una subdivisión de los distintos algoritmos en dos grandes grupos, por un lado se encuentran los **algoritmos criptográficos ultraligeros**, que se enfocan en construir algoritmos de alto rendimiento, orientado a áreas muy específicas. Y por el otro lado los **algoritmos criptográficos ubicuos**, donde entran algoritmos mucho más versátiles, que se ejecutan de forma eficiente en múltiples plataformas, además de que permiten realizar implementaciones más específicas orientadas a evitar posibles ataques que vulneren la seguridad de los mecanismos de encriptación.

8. Hacer un listado ordenado alfabéticamente con toda la bibliografía que han empleado. Para ello, utilizar las normas APA para las citas y referencias bibliográficas.

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].

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. (s.f.). Stream Ciphers livianos estandarizados mediante normas internacionales para ser usados en Internet de las Cosas. *Sistemas, Cibernética e Informática*, *15*(2-2018).

[7] Los ataques de claves relacionadas son un tipo de ataque criptográfico en el cual se intenta comprometer la seguridad en el cifrado aprovechándose de la relación existente entre las diferentes claves utilizadas en el sistema. Estos ataques se basan en el hecho de que ciertos algoritmos criptográficos pueden exhibir vulnerabilidades cuando se utilizan claves relacionadas de alguna manera específica.

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)*.