Preparación de Artículos revista Vínculos: Ciencia, Tecnología y Sociedad
Fecha de envío: 12/09/2022
Fecha de recepción: 18/09/2022
Fecha de aceptación: 09/11/2022

Algoritmo internacional de cifrado de datos (IDEA) que utiliza la variante de cifrado SHA-256

International data encryption algorithm (IDEA) using SHA-256 encryption variant

Anderson Smith Arévalo-Rodríguez[1], Diana Marcela Hurtado-Gómez[2], Gilber Jhon Galindo-Sierra[3]

Resumen: El algoritmo internacional de cifrado de datos fue descrito en 1991, llego para el remplazo de algoritmo DES, este algoritmo cuenta con una seguridad mucho más adaptable y consumiendo menos recursos tecnológicos que el DES, cabe aclarar que para el desarrollo de este algoritmo la criptografía paso por un camino de desarrollo bastante extenso, cabe aclarar que la criptografía se basa en las matemáticas y como mediante esta se protege la información, además de esto siempre se pretende mejorar las protecciones existentes o mezclar tecnologías de encriptación de esta manera resguardar los datos de manera eficiente.

Palabras clave: IDEA, Encriptación, Criptografía, Algoritmo, SHA-256

Abstract: The international data encryption algorithm was described in 1991, it came to replace the DES algorithm, this algorithm has a much more adaptable security and consuming less technological resources than DES, it should be noted that for the development of this algorithm cryptography went through a fairly extensive development path, it should be noted that cryptography is based on mathematics and how this protects the information, besides this is always intended to improve existing protections or mix encryption technologies in this way to protect the data efficiently.

Keywords: IDEA, Encryption, Cryptography, Algorithm, SHA-256.

1. Introducción

El cifrado de mensajes se ha practicado durante más de 4000 años y el origen exacto de la palabra cifrado está en griego (krypto, «oculto», y graphos, «escribir»). La comunicación

[1] Ingeniería en Telemática, Universidad Distrital Francisco José de Caldas, Bogotá, Colombia.
[2] Ingeniería en Telemática, Universidad Distrital Francisco José de Caldas, Bogotá, Colombia.
[3] Ingeniería en Telemática, Universidad Distrital Francisco José de Caldas, Bogotá, Colombia.

está encriptada cuando solo el remitente y el receptor pueden extraer información del mensaje, es decir, una persona fuera de la comunicación solo podrá ver datos sin sentido y el contenido del mensaje estará completamente oculto para ellos.

El cifrado siempre ha ayudado a las civilizaciones a comerciar a comunicar mensajes de política e incluso a ganar guerras, dentro de los principales cifrados de la antigüedad se pueden encontrar los papiros de genbeta, también el cifrado del emperador, incluso tienen tanto impacto que el escritor Homero en una de sus novelas, un hecho historia de la época moderna es como el cifrado generado por los alemanes por poco hace que ganaran la guerra, durante esta el ejército nazi tenido dominado el mar del norte, ya que las comunicaciones que realizaban se hacían por medio de un cifrado y el ejército aliado no encontraba forma de como descifrarlo, gracias a la ayuda de Alan Turing uno de los creadores de los primeros ordenadores pudieron romper el cifrado de estos mensajes generados por la máquina enigma, acá juega un papel muy importante, ya que el cifrado de los mensajes se realizaba por medio de una palabra semilla.

Con el paso del tiempo el propósito se convirtió en mejorar estos algoritmos de cifrado llegando al punto de IDEA en la década de los 90 donde se implementa por medio de movimientos binarios y operaciones lógicas, con esto generando un algoritmo de uso internacional por su eficacia.

Para muchas personas, este es el mejor y más seguro algoritmo simétrico disponible en la actualidad. Funciona con bloques de 64 bits y usa una clave de 128 bits. Como en el caso de DES, se utiliza el mismo algoritmo tanto para el cifrado como para el descifrado. IDEA es un algoritmo bastante seguro, que hasta ahora ha demostrado ser resistente a muchos ataques, incluido el criptoanálisis diferencial. No tiene claves débiles y su longitud de clave hace que un ataque de fuerza bruta sea prácticamente imposible. Como con todos los cifrados de bloques idénticos, IDEA se basa en los conceptos de confusión y difusión.

2. Funciones del algoritmo IDEA

Este algoritmo cumple las funciones principales de cualquier algoritmo dedicado a cifrar información, pero con la garantía que tiene un nivel de protección adecuado, de esta manera que las personas o en la implementación que se realice puede contar con la posibilidad de que su información no caerá en las manos inadecuadas, claro está que ningún sistema es totalmente infalible, pero su complicado método de encripta miento ayuda a evitar este problema de ataques.

2.1.Confidencialidad

En otras palabras, asegura que la información sea accesible solo para personas autorizadas. Para lograr esto, se utilizan tokens y técnicas de encriptación.

2.2.Autenticación

Es decir, proporciona mecanismos que permiten verificar la identidad del comunicador. Para conseguirlo puede usar por ejemplo función hash criptográfica MAC o protocolo de conocimiento cero.

2.3.Integridad

En otras palabras, garantiza la exactitud e integridad de la información. Puede hacer esto usando, por ejemplo, las funciones de hash criptográficas MDC, Bit Interaction Protocol o Electronic Authentication Protocol.

2.4.No rechazo

Permite vincular un documento o transacción a una persona o un sistema de gestión criptográfico automatizado. Cuando se trata de alguien, se trata de asegurarse de que respete ese enlace (compromiso de contenido) para que se entienda que un enlace coordinado incluye una comprensión de sus implicaciones por parte de esa persona. En el pasado, el término "no repudio" utilizado se ha eliminado porque se refiere a conceptos legales que no pueden resolverse únicamente con la tecnología. Con respecto a este término, se entiende que se brinda protección a cualquier entidad involucrada en la comunicación, de manera que indudablemente participa en la totalidad o parte de la comunicación. Para hacer esto, puede utilizar una firma digital, por ejemplo. En algunos contextos, lo que se intenta es todo lo contrario: se puede negar la conexión. Por ejemplo, cuando se utiliza un servicio de mensajería instantánea y no se quiere mostrar esta conexión. Para ello se utilizan técnicas como el cifrado de negación.

3. Seguridad

3.1.Fuerza Bruta

Un ataque de fuerza bruta es un intento de encontrar una contraseña o nombre de usuario, o encontrar un sitio web o una clave oculta que se utiliza para cifrar mensajes, mediante prueba y error, con la esperanza de hacerlo bien. Este es un método de ataque antiguo, pero sigue siendo eficaz y popular entre los piratas informáticos.

Dependiendo de la longitud y complejidad de la contraseña, puede tomar desde unos segundos hasta años para descifrarla. De hecho, según IBM, muchos piratas informáticos atacan el mismo sistema todos los días durante meses o incluso años.

3.2.Criptoanálisis Diferencial

El análisis de tokens o criptoanálisis es el nombre que se le da a varios métodos de ataque criptográfico en cifrados de bloque mediante un conocido ataque de texto sin

formato. El criptoanálisis funciona cifrando texto plano o texto plano conocido, utilizando una clave de cifrado elegida para determinar cómo funciona el cifrado. Se eligen dos entradas con una diferencia fija entre ellas, ya que la diferencia entre las dos entradas se puede determinar utilizando diferentes operaciones, incluida la operación de propiedad OR (XOR).

Cuando el par de entrada pasa por el código de análisis diferencial, el par de salida se configura con la clave de cifrado. La entrada es conocida, por lo que el codificador busca patrones de cambio en la salida.

En primer lugar, un ataque de fuerza bruta no es práctico, ya que se deben verificar 1034 claves, un número que no se puede controlar con los medios aritméticos actuales. Los diseñadores analizaron IDEA para evaluar su fortaleza frente al análisis de codificación diferencial y concluyeron que es inmune a ciertas suposiciones. No se informaron debilidades con respecto al criptoanálisis lineal o algebraico. Se encuentran muchas claves débiles, que rara vez se utilizan en la práctica y deben evitarse explícitamente. Muchos lo consideran uno de los cifrados de bloques más seguros del mercado.

4. Cifrado asimétrico

La seguridad de un sitio web depende de muchos aspectos, incluido el uso de cifrado al enviar información como contraseñas, compartir archivos o transferir otros datos confidenciales.

La criptografía asimétrica (o criptografía de clave pública) permite el establecimiento de una conexión segura entre dos partes, la autenticación mutua de ambas partes y la transmisión de información entre las dos.

El sistema utiliza dos claves para cifrar los mensajes: una clave pública y una clave privada. Para cifrar un mensaje, debe utilizar la clave pública del destinatario (conocida a priori) y la clave privada del remitente. Para descifrarlo, utilice la clave pública del remitente (enviada con el mensaje cifrado) y la clave privada del destinatario. La clave privada es secreta y es la única clave permitida para descifrar el mensaje.

Lo que se pretende lograr es que, si se intercepta el mensaje, ningún tercero pueda descifrar el mensaje.

El concepto de criptografía asimétrica se utiliza desde 1975. Teniendo en cuenta que la historia de la criptografía se remonta a más de 2.000 años, es por ello que este campo se considera muy joven. La mayor ventaja de la criptografía de clave pública es también la mayor desventaja del cifrado simétrico: ambas partes en la comunicación no necesitan compartir una clave pública, pero todos tienen una clave privada diferente.

El método de la clave secreta o cifrado simétrico esconde un problema que existe primero en el intercambio de claves: dado que el receptor debe conocer la clave secreta, cuantos más participantes compartan la clave en la comunicación, más caótica y complicada, y por tanto más. Esta comunicación se vuelve insegura y frágil.

El cifrado asimétrico es una alternativa muy práctica a este método, porque cada usuario tiene su propio par de claves.

4.1.Funcionamiento del cifrado asimétrico

Para iniciar el proceso de cifrado asimétrico, el destinatario genera su par de claves y comunica la clave pública a la otra parte, conservando la clave privada para sí mismo. El

proceso de transmisión es muy simple, a través de una autoridad de certificación o el llamado servidor de claves, donde se puede almacenar la clave. El remitente utiliza esta clave pública para cifrar su mensaje y puede enviarlo al destinatario como un "texto secreto". Desde el momento del cifrado, el destinatario solo podrá descifrar el mensaje utilizando su clave privada. Por este motivo, en principio, puedes elegir libremente el canal del mensaje: si se intercepta un mensaje cifrado, su contenido sigue oculto al atacante.

Este principio unidireccional constituye todo el sistema criptográfico asimétrico. Estas dos claves son completamente independientes: incluso si el atacante conoce la clave pública, no lo ayudará a encontrar la clave privada. Para garantizar esto, la clave pública se multiplica por un número primo bien definido y da un resultado específico. Por ejemplo, utilice el siguiente cálculo:

163 x 367 = 59821

En cuanto a la clave privada, utiliza exclusivamente el resultado de este cálculo (en el ejemplo, el número 59821). Es casi imposible encontrar un número anterior con solo este valor, porque la combinatoria es muy complicada. Hasta el momento, no existe ningún método matemático o algoritmo que facilite los cálculos anteriores.

4.2.Algoritmo SHA-256

En SHA-256 de funciones hash el mensaje de longitud variable M es dividido en bloques de 512 bits M0, M1,...,Mn-1. El valor hash de 256 bits Vn se da la siguiente manera que es la fórmula para encriptación de algoritmo SHA-256 [1].

$$V_0 = IV;\ V_{s+1} = \texttt{compress}(V_s, M_s) = E_{M_s}(V_s) + V_s\ for\ 0 \leq s < n,$$

4.3.Funcionamiento del algoritmo idea utilizando encriptación HASH SHA-256

El algoritmo de cifrado de datos internacional o (IDEA) es un cifrado de bloque de claves simétrico que utiliza un texto plano de longitud fija de 16 bits y los cifra en 4 trozos de 4 bits cada uno para producir texto cifrado de 16 bits. La longitud de la clave utilizada es de 32 bits. La clave también se divide en 8 bloques de 4 bits cada uno[1]. Basándonos en este planteamiento se pueden cifrar cadenas de caracteres de hasta 128 bits realizando una segmentación

Este algoritmo implica una serie de 4 rondas completas idénticas y una media ronda. Cada ronda completa implica una serie de 14 pasos que incluyen operaciones como

Operación XOR

Suma módulo (2^4)

Multiplicación módulo (2^4) +1

Para el caso en el que no se puede hacer la operación modular multiplicación debido a que como resultado no se obtiene un número de 4 bits (un número mayor a 1111) es necesario realizar la operación Multiplicación módulo (2^4) para la encriptación.

Después de 4 rondas completas, la "media ronda" final consta sólo de los 4 primeros pasos de los 14 utilizados anteriormente en las rondas completas. Para realizar estas rondas, cada notación binaria debe convertirse a su notación decimal equivalente, realizar la operación y el resultado obtenido debe convertirse de nuevo a la representación binaria para el resultado final de ese paso concreto.

En la figura 1 se visualizan los pasos a seguir durante cada ronda para esta aplicación del algoritmo IDEA.

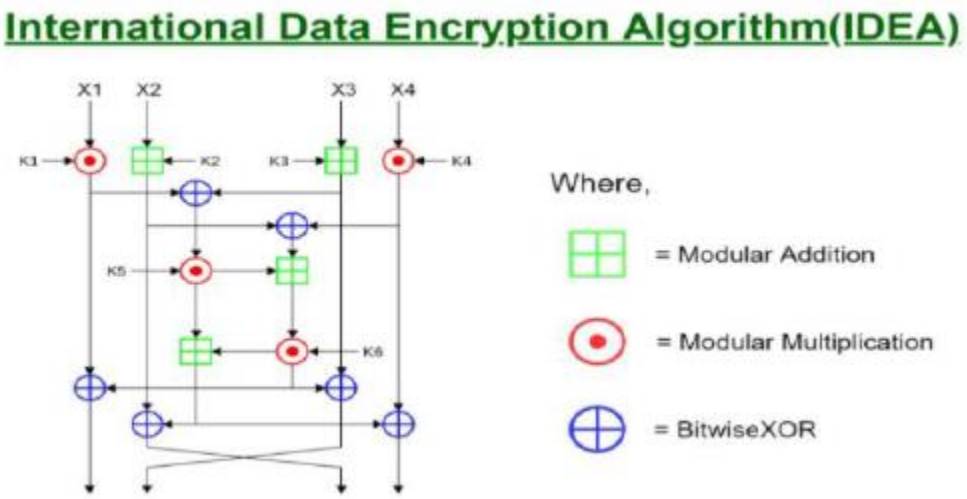

Figura 1. Diagrama algoritmo IDEA. [5]

1. Multiply X_1 and the first subkey Z_1.
2. Add X_2 and the second subkey Z_2.
3. Add X_3 and the third subkey Z_3.
4. Multiply X_4 and the fourth subkey Z_4.
5. Bitwise XOR the results of steps 1 and 3.
6. Bitwise XOR the results of steps 2 and 4.
7. Multiply the result of step 5 and the fifth subkey Z_5.
8. Add the results of steps 6 and 7.
9. Multiply the result of step 8 and the sixth subkey Z_6.
10. Add the results of steps 7 and 9.
11. Bitwise XOR the results of steps 1 and 9.
12. Bitwise XOR the results of steps 3 and 9.
13. Bitwise XOR the results of steps 2 and 10.
14. Bitwise XOR the results of steps 4 and 10.

Figura 2. Pasos para cada una de las rondas algoritmo IDEA. [6]

En la figura 1 se logra identificar las entradas y salidas de cada una de las rondas junto con las operaciones a realizar definidas por el algoritmo, en la figura 2 se observa el paso a paso estas mismas operaciones de manera resumida para llevar a cabo el proceso de encriptación.

4.3.1. Construcción de llaves para cada ronda

En cada ronda completa se utilizan 6 subclaves de 4 bits de las 8 subclaves, mientras que en la media ronda se utilizan 4. Por tanto, 4,5 rondas requieren 28 subclaves. La clave dada, "K", da directamente las primeras 8 subclaves. Rotando la clave principal a la izquierda en 6 bits entre cada grupo de 8, se crean otros grupos de 8 subclaves, lo que implica menos de una rotación por ronda para la clave (3 rotaciones).

4.3.2. Aplicación de encriptación HASH SHA-256

Tras completar las rondas del Algoritmo IDEA y obtener el texto plano cifrado se aplica el algoritmo de encriptación HASH SHA-256 para brindar más seguridad aun al proceso de encriptación obteniendo como resultado nuestro mensaje cifrado.

De esta forma se obtiene el siguiente proceso para aplicar el algoritmo de encriptación completo.

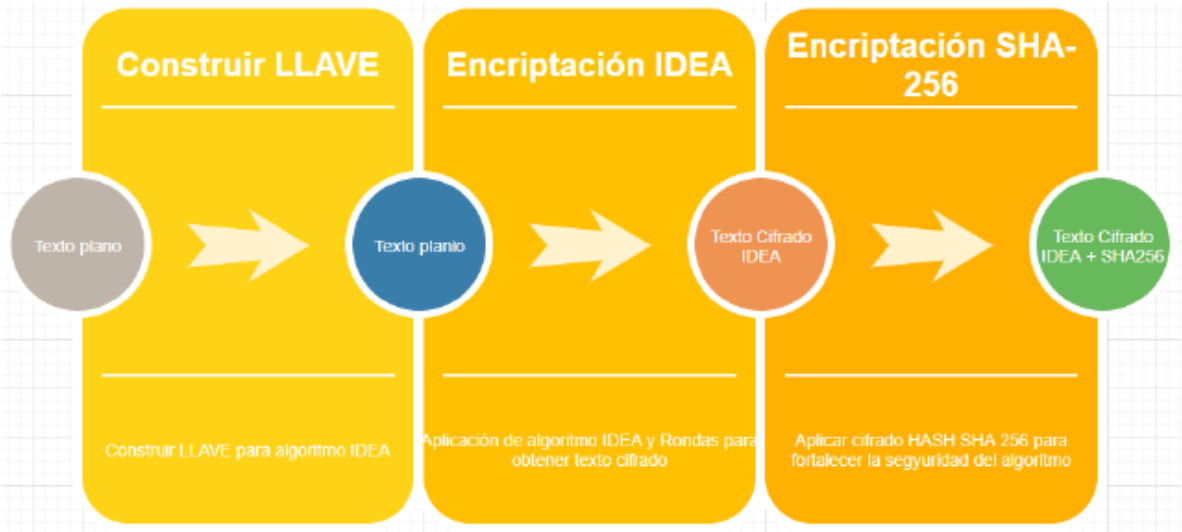

Figura 3. Proceso de encriptación IDEA y SHA-256. [8]

4.3.3. Desencriptación del mensaje

Para desencriptar este mensaje es necesario realizar el proceso a la inversa, primero se desencripta el mensaje convertido en SHA256 y a partir de allí se aplica el proceso de descripción del algoritmo IDEA el cual consiste en realizar los mismos pasos mencionados para la encriptación.

5. Conclusiones

El cifrado o cifrado de mensajes ayuda a que la comunicación sea más segura, y esto también se comprueba cuando se aplica a Internet.

El cifrado de dos claves es un método de cifrado que utiliza un par de claves para enviar mensajes. Estas dos claves pertenecen a la misma persona que recibirá el mensaje. Una clave es pública y puede ser entregada a cualquier persona, la otra clave es privada y el propietario debe conservarla para que nadie pueda acceder a ella. Además, el método criptográfico garantiza que dicho par de claves solo se puede generar una vez, por lo que se puede suponer que es imposible que dos personas obtengan el mismo par de claves de forma casual.

Cabe resaltar que la criptografía de clave pública necesita establecer la confianza correcta de la clave pública del usuario, es decir, la única persona que tiene la clave privada correspondiente es el usuario real al que pertenece.

Referencias

[1] H. Yoshida, "Analysis of a SHA-256 Variant," in Proceedings of the 10th International Conference on Information Security Applications, 2005, pp. 183-194. https://doi.org/10.1007/11693383_17

[2] N. Hoffman, "A Simplified IDEA Algorithm," Semantic Scholar, 2007. Available: https://www.semanticscholar.org/paper/A-Simplified-IDEA-Algorithm-Hoffman/958dc5bf136873fad691987900ec7a0ff5fa737c

[3] V. Beletskyy, "Parallelization of the IDEA Algorithm," in Parallel Computing Technologies, 2004, pp. 1044-1051. https://doi.org/10.1007/978-3-540-24685-5_108

[4] P. Rakheja, "Integrating DNA Computing in International Data Encryption Algorithm (IDEA)," International Journal of Computer Applications, vol. 26, no. 3, 2011, pp. 19-22. https://doi.org/10.5120/3087-4229

[5] Universidad VIU, "¿Qué es la criptografía y cuáles son sus usos?", 2022. Available: https://www.universidadviu.com/es/actualidad/nuestros-expertos/que-es-la-criptografia-y-cuales-son-sus-usos

[6] EcuRed, "International Data Encryption Algorithm (IDEA)", 2011. Available: https://www.ecured.cu/International_Data_Encryption_Algorithm_(IDEA)

[7] Kaspersky, "¿Qué es un ataque de fuerza bruta?," latam.kaspersky.com, Jan. 13, 2021. Available: https://latam.kaspersky.com/resource-center/definitions/brute-force-attack

[8] E. Enrique, "¿Qué es el criptoanálisis diferencial?," QueSignificado.org, Nov. 30, 2020. Available: https://quesignificado.org/que-es-el-criptoanalisis-diferencial/