UNIVERSIDAD DISTRITAL
FRANCISCO JOSÉ DE CALDAS

Revista Vínculos

https://revistas.udistrital.edu.co/index.php/vinculos/

I+D Investigación y Desarrollo

Algoritmo internacional de cifrado de datos (IDEA) con 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]

Para citar este artículo: A. S. Arévalo-Rodríguez, D. M. Hurtado-Gómez, G. J. Galindo-Sierra, "Algoritmo internacional de cifrado de datos (IDEA) con variante de cifrado SHA 256", Revista Vínculos, vol 19, no. 2, pp 107-115, 2022. https://doi.org/10.14483/2322939X.20826

Recibido: 02-03-2022 / Aprobado: 20-05-2022

Resumen: El algoritmo internacional de cifrado de datos fue descrito en 1991, llegó para reemplazar al algoritmo DES. Este algoritmo cuenta con una seguridad mucho más adaptable y consume menos recursos tecnológicos que el DES, cabe destacar que el desarrollo de este algoritmo fue el resultado de un extenso camino de desarrollo en el campo de la criptografía, es importante mencionar que la criptografía se fundamenta en conceptos matemáticos, los cuales son utilizados para proteger la información, además, siempre se busca mejorar las protecciones existentes o mezclar tecnologías de encriptación para 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

1 Ingeniería Telemática, Universidad Distrital Francisco José de Caldas, Colombia
2 Ingeniería Telemática, Universidad Distrital Francisco José de Caldas, Colombia
3 Ingeniería Telemática, Universidad Distrital Francisco José de Caldas, Colombia

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.

1. Introducción

La El cifrado de mensajes ha sido practicado durante más de 4000 años y el origen exacto de la palabra "cifrado" proviene del griego *krypto* que significa "oculto", y *graphos* que significa "escribir". La comunicación se considera encriptada cuando solo el remitente y el receptor pueden extraer información del mensaje, lo que significa que una persona ajena de la comunicación solo podrá ver datos sin sentido y el contenido del mensaje estará completamente oculto para ellos.

A lo largo de la historia, el cifrado siempre ha ayudado a las civilizaciones en el comercio, la comunicación de mensajes políticos e incluso para ganar guerras. Entre los principales cifrados de la antigüedad se encuentran los papiros de Genbeta y el cifrado del emperador que tuvieron un impacto significativo, un ejemplo histórico relevante es cómo el cifrado utilizado por los alemanes casi les permite ganar la guerra, ya que su dominio del Mar del Norte se vio facilitado por las comunicaciones cifradas que el ejército aliado no podía descifrar. Gracias a la ayuda de Alan Turing uno de los creadores de los primeros ordenadores, pudieron romper el cifrado de los mensajes generados por la máquina Enigma, ya que el cifrado de los mensajes se realizaba por medio de una palabra semilla.

Con el tiempo el objetivo se ha centrado en mejorar estos algoritmos de cifrado llegando al desarrollo 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, IDEA es considerado el mejor y más seguro algoritmo simétrico disponible en la actualidad. Funciona con bloques de 64 bits y utiliza una clave de 128 bits. Al igual que con el DES, el mismo algoritmo se utiliza tanto para el cifrado como para el descifrado. IDEA ha demostrado ser bastante seguro, y resistente a diversos ataques, incluido el criptoanálisis diferencial. Su longitud de clave y la ausencia de claves débiles hacen que sea prácticamente imposible llevar a cabo un ataque de fuerza bruta. Al igual que con

todos los cifrados de bloques idénticos, IDEA se basa en los principios de confusión y difusión.

1.1 Funciones del algoritmo IDEA

Este algoritmo cumple con las funciones principales de cualquier algoritmo dedicado al cifrado de información, con la garantía de proporcionar un nivel adecuado de protección. De esta manera, las personas o las implementaciones que lo utilicen pueden confiar en que su información no caerá en manos indebidas, es importante tener en cuenta que ningún sistema es totalmente infalible, pero su complejo método de encriptación ayuda a mitigar el riesgo de ataques.

Confidencialidad

En otras palabras, garantiza que la información solo sea accesible para personas autorizadas. Para lograrlo, se emplean tokens y técnicas de encriptación.

Autenticación

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

Integridad

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

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), lo que implica que comprenda las implicaciones de dicho enlace. El término "no repudio" utilizado en el pasado, se ha eliminado porque se refiere a conceptos legales que no pueden abordarse únicamente con tecnología. En cambio, se entiende que se brinda protección a cualquier entidad involucrada en la comunicación, asegurando su participación inequívoca en la totalidad o parte de la comunicación. Esto puede lograrse mediante el uso de una firma digital, por ejemplo. En algunos contextos el objetivo es lo contrario: negar la conexión, como cuando utilizamos un servicio de mensajería instantánea y no queremos mostrar esta conexión. Para ello se utilizan técnicas como el cifrado de negación.

ISSN 1794-211X • e-ISSN 2322-939X • Vol 19, N° 2 (julio-diciembre 2022). pp. 107-115. Universidad Distrital Francisco José de Caldas-Facultad Tecnológica.

1.2 Seguridad

Fuerza Bruta

Un ataque de fuerza bruta es un intento de encontrar una contraseña, nombre de usuario, sitio web o clave oculta utilizada para cifrar mensajes, mediante prueba y error, con la esperanza de encontrar la combinación correcta. Aunque es un método de ataque antiguo, sigue siendo eficaz y popular entre los piratas informáticos.

El tiempo necesario para descifrar una contraseña mediante un ataque de fuerza bruta depende de su longitud y complejidad. Puede variar desde unos segundos hasta años. De hecho, según IBM, muchos piratas informáticos continúan atacando el mismo sistema todos los días durante meses o incluso años.

Criptoanálisis Diferencial

El análisis de tokens o criptoanálisis es el término utilizado para describir varios métodos de ataque criptográfico en sistemas de cifrado 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 algoritmo de cifrado. Se eligen dos entradas con una diferencia fija entre ellas, ya que la variación entre estas entradas se puede determinar utilizando diferentes operaciones, como la operación de propiedad OR (XOR). Al pasar este par de entradas por el código de análisis diferencial, el par de salida se configura con la clave de cifrado. Dado que la entrada es conocida, el codificador busca patrones de cambio en la salida para inferir información sobre la clave utilizada en el proceso de cifrado.

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. Aunque se han identificado algunas claves débiles, estas son poco utilizadas en la práctica y deben evitarse explícitamente. En general, IDEA es considerado uno de los cifrados de bloques más seguros del mercado.

2. Cifrado asimétrico

La seguridad de un sitio web depende de muchos aspectos, entre ellos el uso de cifrado al enviar información confidencial como contraseñas, o archivos compartidos.

La criptografía asimétrica, también conocida como criptografía de clave pública, permite establecer una conexión segura entre dos partes, autenticar mutuamente a ambas partes y transmitir información entre las ellas.

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, se utiliza 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.

El concepto de criptografía asimétrica nació en 1975, lo que la convierte en un campo relativamente joven en comparación con la historia milenaria de la criptología que se remonta a más de 2.000 año. Su principal ventaja radica en que no es necesario que las partes compartan una clave secreta, pero todas tienen una clave privada diferente, lo que garantiza una mayor seguridad en la comunicación.

En contraste el método de la clave secreta o cifrado simétrico esconde un problema en el intercambio de claves, ya que cuanto más compleja sea la comunicación y más participantes compartan la misma clave, mayor será el riesgo de que la comunicación se vuelva insegura. El cifrado asimétrico ofrece una solución práctica a este problema al asignar a cada usuario su propio par de claves.

3. 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 de manera segura. 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, se puede 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:

$$163 \times 367 = 59821$$

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.

ISSN 1794-211X • e-ISSN 2322-939X • Vol 19, N° 2 (julio-diciembre 2022). pp. 107-115. Universidad Distrital Francisco José de Caldas-Facultad Tecnológica.

4. Algoritmo SHA 256

ShA-256 de funciones hash ([17], p. 341). 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 de la siguiente manera:

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

4.1 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]. Basando en este planteamiento se puede 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:

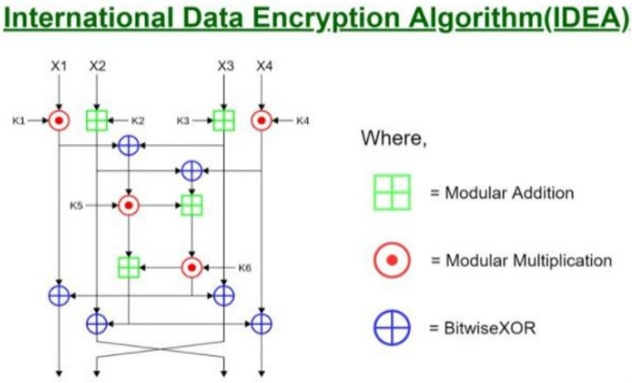
Operación XOR
Suma módulo (2^4)
Multiplicación módulo (2^4)+1

Para el caso en el que no se puede hacer la operación modular multiplicación debido a que como resultado no obtenemos 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 las Figuras 1 y 2 se visualizan los pasos a seguir durante cada ronda para esta aplicación del algoritmo IDEA.

Figura 1. Diagrama algoritmo IDEA



Fuente: Elaboración propia.

ISSN 1794-211X • e-ISSN 2322-939X • Vol 19, N° 2 (julio-diciembre 2022). pp. 107-115. Universidad Distrital Francisco José de Caldas-Facultad Tecnológica.

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

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.

Fuente: Elaboración propia.

En la Figura 1 logramos 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 podemos observar paso a paso estas mismas operaciones de manera resumida para llevar a cabo el proceso de encriptación.

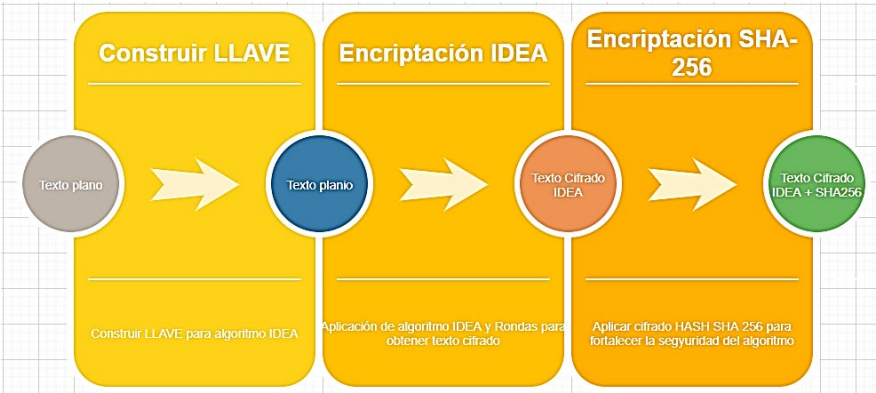
4.2 Construcción de llaves para cada ronda

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 Aplicación de encriptación HASH SHA-256

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

Figura 3. Proceso de encriptación IDEA y SHA-256.



Fuente: Elaboración propia.

ISSN 1794-211X • e-ISSN 2322-939X • Vol 19, N° 2 (julio-diciembre 2022). pp. 107-115. Universidad Distrital Francisco José de Caldas-Facultad Tecnológica.

De esta forma obtenemos el proceso en la Figura 3 para aplicar el algoritmo de encriptación completo.

4.4 Desencriptación del mensaje

Para desencriptar este mensaje es necesario realizar el proceso a la inversa, primero desencriptamos el mensaje convertido en SHA-256 y a partir de allí aplicamos 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, también 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 señalar 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 _SpringerLink_, Aug. 11, 2005. https://link.springer.com/chapter/10.1007/11693383_17?error=cookies_not_supported&code=18cc071b-4ac6-493e-8a1e-e9ad6288d0e7

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

[3] V. Beletskyy, "Parallelization of the IDEA Algorithm," in _SpringerLink_, Jun. 6, 2004. https://link.springer.com/chapter/10.1007/978-3-540-24685-5_108?error=cookies_not_supported&code=cd20503e-d021-41f6-9f5b-f52d18beac5c

[4] P. Rakheja, "Integrating DNA Computing in International Data Encryption Algorithm (IDEA),"

International Journal of Computer Applications - IJCA, 2011. https://doi.org/10.5120/3087-4229

[5] Amazon AWS, "¿Qué es la criptografía?," 2020. https://aws.amazon.com/es/what-is/cryptography/

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

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

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