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

I+D Investigación y Desarrollo

IDEA: Algoritmo Criptográfico Simétrico para la Protección Segura de Datos Sensibles

IDEA: Symmetric Cryptographic Algorithm for Secure Protection of Sensitive Data

Jairo Guerrero-Reyes [1], Claudia Rodríguez-Martínez [2]

Para citar este artículo: J. Guerrero-Reyes, C. Rodríguez-Martínez "IDEA: Algoritmo Criptográfico Simétrico para la Protección Segura de Datos Sensibles", Revista Vínculos, vol 20, no. 2, pp 116-124, 2023. https://doi.org/10.14483/2322939X.20826

Resumen: El International Data Encryption Algorithm (IDEA) es un cifrador de bloques simétrico desarrollado en 1991 por Xuejia Lai y James Massey. Este algoritmo opera sobre bloques de 64 bits utilizando una clave de 128 bits, y es conocido por su alta resistencia a los ataques criptográficos. IDEA se basa en una combinación de operaciones matemáticas—suma modular, multiplicación modular y XOR—que se aplican a lo largo de 8.5 rondas de procesamiento. Estas operaciones permiten que incluso las variaciones mínimas en los datos de entrada o en la clave generen resultados significativamente diferentes, lo que se traduce en una robusta seguridad criptográfica. La estructura del algoritmo sigue un esquema de Feistel modificado, donde el bloque de datos se divide en partes, se procesa a través de varias rondas de transformación, y se vuelve a combinar para formar el bloque cifrado final. Además, la generación de subclaves a partir de la clave principal añade una capa extra de seguridad.

El éxito de IDEA en la criptografía se refleja en su implementación en aplicaciones críticas, como PGP (Pretty Good Privacy), donde se utiliza para cifrar correos electrónicos y asegurar comunicaciones electrónicas. A lo largo de los años, IDEA ha demostrado ser eficaz contra ataques como el criptoanálisis diferencial y lineal, lo que lo convierte en una opción segura para la protección de datos. Aunque con el

1 SENA. E-mail: jairogueres@gmail.com
2 SENA. E-mail: crodriguez311@gmail.com

tiempo han surgido nuevos algoritmos que han desplazado a IDEA en algunas aplicaciones, su diseño sigue siendo relevante y estudiado en la criptografía moderna. Este artículo proporciona una visión detallada del funcionamiento de IDEA, su estructura y su importancia en el campo de la seguridad de la información, destacando su capacidad para ofrecer un cifrado seguro y eficiente en una amplia gama de contextos.

Palabras clave: Algoritmo IDEA, cifrado simétrico, seguridad criptográfica, generación de subclaves.

Abstract

The International Data Encryption Algorithm (IDEA) is a symmetric block cipher developed in 1991 by Xuejia Lai and James Massey. This algorithm operates on 64-bit blocks using a 128-bit key and is known for its high resistance to cryptographic attacks. IDEA is based on a combination of mathematical operations-modular addition, modular multiplication and XOR-which are applied over 8.5 processing rounds. These operations allow even minute variations in the input data or key to generate significantly different results, resulting in robust cryptographic security. The structure of the algorithm follows a modified Feistel scheme, where the data block is split into parts, processed through several rounds of transformation, and re-combined to form the final cipher block. In addition, the generation of subkeys from the main key adds an extra layer of security.

IDEA's success in cryptography is reflected in its implementation in critical applications, such as PGP (Pretty Good Privacy), where it is used to encrypt emails and secure electronic communications. Over the years, IDEA has proven effective against attacks such as differential and linear cryptanalysis, making it a secure option for data protection. Although new algorithms have emerged over time that have displaced IDEA in some applications, its design remains relevant and studied in modern cryptography. This article provides a detailed overview of IDEA's operation, its structure, and its importance in the field of information security, highlighting its ability to provide secure and efficient encryption in a wide range of contexts.

Keywords: IDEA Algorithm, symmetric encryption, cryptographic security, subkey generation.

1. Introducción

En un mundo cada vez más digitalizado, la seguridad de la información se ha convertido en una prioridad fundamental. La criptografía, el arte de proteger datos mediante técnicas matemáticas, juega un papel crucial en asegurar la integridad y confidencialidad de la información que circula a través de redes y sistemas de

almacenamiento. Uno de los algoritmos que ha sido ampliamente reconocido por su solidez y eficacia en este campo es el International Data Encryption Algorithm (IDEA).

Desarrollado en 1991 por los criptógrafos Xuejia Lai y James Massey en el Instituto Federal Suizo de Tecnología en Zúrich, IDEA se diseñó como un sucesor mejorado del Data Encryption Standard (DES), que en ese momento comenzaba a mostrar vulnerabilidades frente a los avances en técnicas de criptoanálisis y la creciente capacidad de cómputo [1], [2]. A diferencia de DES, que utiliza una clave de 56 bits, IDEA emplea una clave de 128 bits, lo que proporciona un espacio de clave mucho mayor y, por ende, una mayor seguridad [3].

IDEA es un cifrador de bloques simétrico que cifra bloques de 64 bits de datos mediante una serie de operaciones matemáticas que incluyen la suma modular, la multiplicación modular y el operador XOR. Estas operaciones se repiten a lo largo de 8.5 rondas, un diseño que permite lograr un alto nivel de difusión y confusión, principios fundamentales para la seguridad en criptografía [4]. La robustez del algoritmo radica en la manera en que estas operaciones no lineales interactúan, asegurando que incluso un pequeño cambio en el texto original o en la clave de cifrado genere un cambio drástico en el texto cifrado, lo que se conoce como el efecto avalancha [5], [6].

El algoritmo ha sido implementado en diversas aplicaciones, siendo notable su uso en Pretty Good Privacy (PGP), un software de cifrado de correos electrónicos ampliamente utilizado [7]. La elección de IDEA en PGP se debe a su capacidad para ofrecer un cifrado seguro sin requerir una gran cantidad de recursos computacionales, lo que lo hace ideal para sistemas de comunicación en tiempo real y dispositivos con limitaciones de procesamiento [8], [9]. Además, IDEA ha sido integrado en sistemas de almacenamiento seguro de datos y en protocolos de seguridad de redes, donde su eficiencia y resistencia a los ataques lo han convertido en una opción confiable [10].

Uno de los aspectos clave de IDEA es su resistencia a ataques criptográficos avanzados como el criptoanálisis diferencial y lineal. Estas técnicas, que se han utilizado para comprometer otros algoritmos, han demostrado ser ineficaces contra IDEA debido a la complejidad y la no linealidad introducida por sus operaciones matemáticas [11], [12]. Además, la generación de subclaves a partir de la clave principal de 128 bits añade un nivel adicional de seguridad, haciendo que sea extremadamente difícil para un atacante derivar la clave original mediante técnicas de fuerza bruta [13].

A pesar de la aparición de nuevos algoritmos como AES (Advanced Encryption Standard), que ha sido adoptado ampliamente en aplicaciones modernas,

ISSN 1794-211X • e-ISSN 2322-939X • Vol 20, N° 2 (julio-diciembre 2022). pp. 116-124. Universidad Distrital Francisco José de Caldas-Facultad Tecnológica.

IDEA sigue siendo relevante y es un tema de estudio en la criptografía moderna [14]. Su diseño elegante y su capacidad para ofrecer un equilibrio entre seguridad y eficiencia han asegurado su lugar en la historia de la criptografía como uno de los algoritmos más importantes y robustos de la era moderna [15].

Este artículo se propone analizar en profundidad el funcionamiento del algoritmo IDEA, su estructura interna, y su aplicación en el campo de la seguridad de la información. A través de esta revisión, se destaca la importancia de IDEA en la evolución de la criptografía y su legado como un pilar en la protección de datos sensibles en un mundo digital en constante evolución.

2. Principios Fundamentales del Algoritmo IDEA

IDEA es un cifrador de bloques simétrico que opera sobre bloques de 64 bits y utiliza una clave de 128 bits. Su seguridad radica en la combinación de tres operaciones matemáticas fundamentales: la suma modular (mod 2^16), la multiplicación modular (mod 2^16 + 1) y el operador XOR. Estas operaciones se aplican en un esquema iterativo de 8.5 rondas, lo que garantiza que cualquier cambio mínimo en los datos de entrada se propague de manera significativa en la salida, dificultando así los ataques criptográficos [1], [4].

2.1.Suma Modular

La suma modular es una operación básica en la que cada bit del bloque de datos se suma con el correspondiente bit de la subclave, con el resultado modulado por 2^16. Esta operación introduce una complejidad adicional al cifrado, ya que la suma no lineal hace que sea difícil predecir el resultado final basado solo en la entrada [2], [3].

2.2.Multiplicación Modular

La multiplicación modular (mod 2^16 + 1) es otra operación clave en IDEA. Esta operación se lleva a cabo entre el valor del bloque de datos y la subclave. La multiplicación modular es más compleja que la suma modular, lo que agrega un nivel adicional de seguridad al algoritmo. Además, cualquier valor de entrada igual a cero se reemplaza por uno, lo que previene la aparición de ceros en la operación final, asegurando que el cifrado no produzca resultados triviales [4], [5].

2.3.XOR (O-exclusivo)

El operador XOR, o O-exclusivo, es una operación bit a bit que combina dos bloques de datos de manera que el resultado sea 1 solo si los bits correspondientes son diferentes. En el contexto de IDEA, el uso de XOR añade una capa más de no linealidad, lo que contribuye a la seguridad del algoritmo al

dificultar los intentos de criptoanálisis lineal [6], [7].

3. Estructura del Algoritmo

El algoritmo IDEA sigue una estructura de Feistel modificada, lo que significa que, en cada ronda el bloque de datos se divide, se procesa y luego se reensambla. Esta estructura permite que el cifrado y el descifrado se realicen de manera similar, utilizando las mismas operaciones, pero aplicando las subclaves en orden inverso durante el descifrado [1], [8].

3.1. División del Bloque

El proceso de cifrado comienza dividiendo el bloque de 64 bits en cuatro sub-bloques de 16 bits. Estos sub-bloques se procesan individualmente a lo largo de las rondas del algoritmo [9].

3.2. Rondas de Transformación

Durante las primeras 8 rondas se aplican las operaciones de suma, multiplicación y XOR utilizando subclaves derivadas de la clave principal de 128 bits. Cada ronda se compone de múltiples pasos en los que los sub-bloques se mezclan y se transforman, lo que incrementa la difusión y la confusión [10].

3.3. Mitad de Ronda Final

La última ronda del algoritmo, conocida como "mitad de ronda", es una ronda parcial que se realiza con operaciones adicionales. Esta ronda finaliza el proceso de difusión completa del bloque, asegurando que cualquier pequeña modificación en los datos de entrada afecte a todo el bloque de salida [11].

3.4. Combinación de los Subbloques

Finalmente, los sub-bloques resultantes se combinan para formar el bloque cifrado final. Este proceso garantiza que el bloque de salida tenga un alto nivel de aleatoriedad, lo que dificulta su análisis y descifrado sin la clave correcta [12].

3.5. Generación de Subclaves

IDEA utiliza un total de 52 subclaves de 16 bits, derivadas de la clave principal de 128 bits. La generación de estas subclaves implica la rotación y selección de bits específicos de la clave principal, lo que añade un nivel adicional de seguridad. Esta rotación asegura que las subclaves sean suficientemente diferentes entre sí, minimizando la posibilidad de ataques basados en patrones repetitivos [13], [14].

ISSN 1794-211X • e-ISSN 2322-939X • Vol 20, N° 2 (julio-diciembre 2022). pp. 116-124. Universidad Distrital Francisco José de Caldas-Facultad Tecnológica.

4. Aplicaciones del Algoritmo IDEA

Desde su introducción, IDEA ha sido adoptado en diversas aplicaciones, siendo la más conocida su implementación en Pretty Good Privacy (PGP), un software utilizado para el cifrado de correos electrónicos. PGP confía en IDEA debido a su capacidad para ofrecer un equilibrio entre seguridad y eficiencia, lo que lo hace ideal para aplicaciones donde la velocidad y la seguridad son críticas [7], [9].

Además de PGP, IDEA ha sido implementado en sistemas de almacenamiento de datos seguros y en protocolos de seguridad de redes. Su resistencia a ataques como el criptoanálisis diferencial y lineal ha asegurado su lugar en sistemas que requieren un alto nivel de protección de datos [15].

5. Resistencia a Ataques Criptográficos

Uno de los aspectos más destacados de IDEA es su resistencia a técnicas de criptoanálisis avanzadas, como el criptoanálisis diferencial y lineal. Estos métodos, que han sido efectivos contra otros algoritmos de cifrado, no han logrado comprometer la seguridad de IDEA debido a su compleja estructura y a la combinación de operaciones no lineales. El efecto avalancha garantizado por IDEA asegura que cualquier pequeño cambio en el texto original o en la clave de cifrado provoque un cambio drástico en el texto cifrado, lo que dificulta el análisis predictivo del cifrado [11], [12]. Se presenta el siguiente código en Python para ejemplificar el algoritmo:

```
def multiplicacion_modular(a, b):
    mod = 2**16 + 1
    if a == 0:
        a = 1
    if b == 0:
        b = 1
    resultado = (a * b) % mod
    if resultado == 0:
        resultado = 1
    return resultado

def suma_modular(a, b):
    return (a + b) % 2**16

def cifrar_bloque(entrada, subclaves):
    x1, x2, x3, x4 = entrada

    for i in range(8):  # 8 rondas
        x1 = multiplicacion_modular(x1, subclaves[6*i])
        x2 = suma_modular(x2, subclaves[6*i + 1])
        x3 = suma_modular(x3, subclaves[6*i + 2])
        x4 = multiplicacion_modular(x4, subclaves[6*i +
3])

        x5 = x1 ^ x3
        x6 = x2 ^ x4

        x7 = multiplicacion_modular(x5, subclaves[6*i +
4])
        x8 = suma_modular(x6, x7)

        x9 = multiplicacion_modular(x8, subclaves[6*i +
5])
        x10 = suma_modular(x7, x9)

        x1 = x1 ^ x9
        x4 = x4 ^ x9
        x2 = x2 ^ x10
        x3 = x3 ^ x10
```


ISSN 1794-211X • e-ISSN 2322-939X • Vol 20, N° 2 (julio-diciembre 2022). pp. 116-124. Universidad Distrital Francisco José de Caldas-Facultad Tecnológica.

```
    # Media ronda final
    x1 = multiplicacion_modular(x1, subclaves[48])
    x2 = suma_modular(x2, subclaves[49])
    x3 = suma_modular(x3, subclaves[50])
    x4 = multiplicacion_modular(x4, subclaves[51])

    return [x1, x3, x2, x4]  # orden de salida diferente
```

6. Conclusiones

El International Data Encryption Algorithm (IDEA) es un hito en la historia de la criptografía moderna. Su diseño robusto y eficiente ha garantizado su uso en aplicaciones críticas durante más de tres décadas. Aunque algoritmos más recientes como AES han ganado popularidad, IDEA sigue siendo relevante en escenarios donde se requiere un alto nivel de seguridad con un rendimiento computacional razonable. Su resistencia a ataques criptográficos y su capacidad para operar eficientemente en diferentes plataformas hacen de IDEA una opción confiable para la protección de datos sensibles.

Este artículo ha explorado en detalle los fundamentos, la estructura y las aplicaciones de IDEA, destacando su importancia en la evolución de la criptografía. A medida que el mundo continúa digitalizándose, la necesidad de algoritmos seguros y confiables como IDEA seguirá siendo esencial para proteger la integridad y la confidencialidad de la información en un entorno digital cada vez más complejo.

Aunque han surgido algoritmos nuevos como AES, IDEA sigue siendo importante en el campo de la criptografía. Su habilidad para resistir técnicas de ataque avanzadas asegura que siga siendo una opción confiable para proteger datos. La implementación de IDEA en diferentes plataformas, desde hardware hasta software, muestra su flexibilidad y utilidad en diversas aplicaciones.

Referencias

[1] Cui, M. “Introduction to the k-means clustering algorithm based on the elbow method,” *Accounting, Auditing and Finance*, vol. 1, no. 1, pp. 5-8, 2020.

[2] H. Jia, X. Peng, & C. Lang, “Remora optimization algorithm,” *Expert Systems with Applications*, vol. 185, p. 115665, 2021.

[3] D. R. Ibrahim, J. S. Teh, & R. Abdullah, “An overview of visual cryptography techniques,” *Multimedia Tools and Applications*, vol. 80, pp. 31927-31952, 2021.

[4] D. K. Sharma, N. C. Singh, D. A. Noola, A. N. Doss, & J. Sivakumar, “A review on various cryptographic techniques & algorithms,” *Materials Today: Proceedings*, vol. 51, pp. 104-109, 2022.

[5] M. Rana, Q. Mamun, & R. Islam, "Lightweight cryptography in IoT networks: A survey," *Future Generation Computer Systems*, vol. 129, pp. 77-89, 2022.

[6] S. M. Hassan, & G. G. Hamza, "Real-time FPGA implementation of concatenated AES and IDEA cryptography system," *Indonesian Journal of Electrical Engineering and Computer Science (ijeecs),* vol. 22, no.1, pp. 71-82, 2021.

[7] V. A. Thakor, M. A. Razzaque, & M. R. Khandaker, "Lightweight cryptography algorithms for resource-constrained IoT devices: A review, comparison and research opportunities," *IEEE Access*, vol. 9, pp. 28177-28193, 2021.

[8] A. Fotovvat, G. M. Rahman, S. S. Vedaei, & K. A. Wahid, "Comparative performance analysis of lightweight cryptography algorithms for IoT sensor nodes," *IEEE Internet of Things Journal*, vol. 8, no.10, pp. 8279-8290, 2020.

[9] C. Portmann, & R. Renner, "Security in quantum cryptography," *Reviews of Modern Physics,* vol. 94, no. 2, p. 025008, 2022.

[10] B. E. H. H. Hamouda, "Comparative study of different cryptographic algorithms," *Journal of Information Security*, vol. 11, no. 3, pp. 138-148, 2020.

[11] Р. О. Султанов, "Idea блокли шифрлаш алгоритмини такомиллаштириш методлари," *Academic Research in Educational Sciences*, vol. 3, no. 397-404. 2020.

[12] D. M. Ruano-Daza, B. D., L. F. Valiente-Simbaqueba, Guevara-Triana, & M. S. P. Poblador, "Análisis del rendimiento entre los algoritmos simétricos de Blowfish y AES," *Revista Vínculos*, vol. 18, no. 2, 2021.

[13] S. Kumar, G. Karnani, M. S. Gaur, & A. Mishra, "Cloud security using hybrid cryptography algorithms," In *2021 2nd international conference on intelligent engineering and management (ICIEM) IEEE*. pp. 599-604, abr, 2021.

[14] F. Grasselli, "Quantum cryptography," *Quantum science and technology*. Cham: Springer, 2021.

[15] H. Abroshan, "A hybrid encryption solution to improve cloud computing security using symmetric and asymmetric cryptography algorithms," *International Journal of Advanced Computer Science and Applications*, vol. 12, no. 6, 2021.

ISSN 1794-211X • e-ISSN 2322-939X • Vol 20, N° 2 (julio-diciembre 2022). pp. 116-124. Universidad Distrital Francisco José de Caldas-Facultad Tecnológica.