Algoritmos de Cifrado Moderno
2023-2

Rojas Terrazas Laylet [*] **Ruiz Sánchez Miguel Ángel** [**]

[*] *Sistemas Operativos*
[**] *Sistemas Operativos*

Resumen: Un algoritmo es un conjunto de operaciones que busca resolver un problema determinado a través de secuencias lógicas, por otro lado, un algoritmo de cifrado es un conjunto de reglas y procedimientos matemáticos que nos ayuda a proteger o asegurar el transporte de información.
Funciones:

- Confidencialidad: codifica el contenido del mensaje.
- Autenticación: verifica el origen de un mensaje.
- Integridad: demuestra que el contenido de un mensaje no ha cambiado desde que se envió.
- No rechazo: evita que los remitentes nieguen haber enviado el mensaje cifrado.

Palabras clave: Algoritmos de cifrado, Simétrico, Asimétrico

1. INTRODUCCIÓN

La historia del cifrado se remonta a la antigua Grecia, donde se utilizaba la técnica de la sustitución de letras, conocida como el cifrado de César. Julio César utilizó este cifrado para enviar mensajes secretos a sus generales. El cifrado de César implica desplazar cada letra del alfabeto por un número fijo de posiciones. A lo largo de la historia, se han desarrollado muchas técnicas diferentes de cifrado, incluyendo el cifrado de sustitución, el cifrado de transposición, el cifrado de clave pública y el cifrado de clave simétrica. En el siglo XIX, se desarrollaron máquinas de cifrado mecánicas, como la Enigma utilizada por el ejército alemán durante la Segunda Guerra Mundial.[1] Hasta mediados de 1970, todos los esquemas de criptografía dependían de una llave única: el equivalente a una contraseña que permitía tanto convertir un texto claro en una representación ininteligible como manipular a dicha representación para obtener de vuelta al texto claro. Entre el breve lapso comprendido 1976 y 1980, el mundo de la criptografía cambió por completo: nació la criptografía de llave pública, con los principales protocolos que siguen siendo utilizados al día de hoy. Esencialmente, en vez de manejar una sola llave, se descubrieron varias funciones matemáticas que permiten llaves compuestas de dos mitades: una privada, que cada individuo debe custodiar celosamente, y una pública, que puede ser ampliamente distribuida. Estas dos llaves actúan como inversas: lo que se cifra con una sólo puede descifrarse con la otra.[2]

2. CIFRADO SIMÉTRICO:

El cifrado simétrico es un método de cifrado en el que se utiliza la misma clave para cifrar y descifrar la información. Es decir, tanto el emisor como el receptor utilizan la misma clave para proteger y acceder a la información cifrada. La clave puede ser tanto una palabra, como un número o una cadena de letras. El proceso de cifrado simétrico implica tomar el mensaje original y la clave de cifrado, y aplicar una serie de operaciones matemáticas para convertir el mensaje original en un mensaje cifrado. El receptor utiliza la misma clave de cifrado para aplicar una serie de operaciones matemáticas inversas para descifrar el mensaje cifrado y volver al mensaje original.

Características importantes:

- El cifrado simétrico es más rápido que el cifrado asimétrico ya que utiliza menos procesamiento y recursos.
- El tamaño del texto en el cifrado simétrico, una vez ha sido cifrado, es igual o más pequeño que el texto sin formato.
- El cifrado simétrico se emplea cuando es necesario transferir una cantidad grande de datos.

A finales de la década de 1970, el cifrado simétrico evolucionó aún más con el desarrollo de los algoritmos de cifrados modernos como el DES (Data Encryption Standard), que se convirtió en el estándar de cifrado simétrico para el gobierno de los Estados Unidos en 1977. Desde entonces, se han desarrollado varios otros algoritmos de cifrado simétrico más fuertes, como AES (Advanced Encryption Standard), que se utiliza ampliamente en la actualidad para proteger la información sensible y las comunicaciones en línea.

Una de las limitaciones del cifrado simétrico es que, como se utiliza la misma clave para cifrar y descifrar, existe el riesgo de que un tercero pueda interceptar la clave y acceder a la información cifrada. (**?**)

3. AES (ADVANCED ENCRYPTION STANDARD)

Es uno de los algoritmos de cifrado más utilizados y seguros actualmente disponibles. Es de acceso público, y es el cifrado que la NSA utiliza para asegurar documentos con la clasificación "top secret". Su historia de éxito se inició en

1997, cuando el NIST (Instituto Nacional de Estándares y Tecnología) comenzó oficialmente a buscar un sucesor al envejecimiento cifrado estándar DES. Un algoritmo llamado Rijndael", desarrollado por los criptografistas belgas Daemen y Rijmen, sobresalía tanto en seguridad como en rendimiento y flexibilidad. Apareció en la cima de varios competidores y se anunció oficialmente el nuevo estándar de cifrado AES en 2001.

El algoritmo se basa en varias sustituciones, permutaciones y transformaciones lineales para convertir el texto plano en texto cifrado, cada una ejecutada en bloques de datos de 16 bytes. Esas operaciones se repiten varias veces, llamadas rondas". Durante cada ronda, una clave circular única se calcula a partir de la clave de cifrado y se incorpora en los cálculos. Basado en la estructura de bloques de AES, el cambio de un solo bit, ya sea en la clave, o en el bloque de texto sin cifrado, da como resultado un bloque de texto cifrado completamente diferente - una ventaja clara sobre los cifrados de flujo tradicionales. La diferencia entre AES-128, AES-192 y AES-256 finalmente es la longitud de la clave: 128, 192 o 256 bits - todas las mejoras drásticas en comparación con la clave de 56 bits de DES.[9]

A modo de ilustración: El agrietamiento de una clave AES de 128 bits el espacio de búsqueda es de 2128 (del orden de 1038) posibilidades., si tuviéramos poder de cómputo suficiente para intentar decodificar un billón de llaves por segundo, una búsqueda exhaustiva tomaría sólo 719 millones de veces la edad del universo. En contraste (e ilustrando el crecimiento exponencial), una llave de 64 bits tomaría sólo 213 días. Hasta el día de hoy, no existe un ataque factible contra AES. Por lo tanto, AES sigue siendo el estándar de cifrado preferido para los gobiernos, bancos y sistemas de alta seguridad en todo el mundo. [3] El algoritmo AES ha demostrado ser altamente seguro y resistente a los ataques de fuerza bruta y otros métodos criptoanalíticos. Además, es muy rápido y eficiente en términos de procesamiento, lo que lo hace ideal para aplicaciones de cifrado en línea y en dispositivos móviles.

4. CIFRADO ASIMÉTRICO:

La criptografía asimétrica es el método criptográfico que usa un par de claves para el envío de mensajes. Las dos claves pertenecen a la misma persona a la que se ha enviado el mensaje. Una clave es pública y se puede entregar a cualquier persona, la otra clave es privada y el propietario debe guardarla de modo que nadie tenga acceso a ella.[7]

Características importantes:

- Da solución a las claves que se cifran y descifran por el mismo canal inseguro (cifrado simétrico)

Desventajas (tarda más)

- Tienen mayor tiempo de procesamiento
- Tardan mas en cifrar teniendo un tamaño mayor a las simétricas

5. ALGORITMO LUKS

LUKS (Linux Unified Key Setup) es un estándar de cifrado de disco completo para sistemas Linux que proporciona una capa adicional de seguridad para la protección de datos. LUKS utiliza el cifrado simétrico y asimétrico para cifrar todo el disco duro o una partición específica y se integra con el sistema operativo para proporcionar una experiencia de usuario transparente. LUKS utiliza el cifrado simétrico para cifrar los datos en el disco. Cuando se crea una partición LUKS, se genera una clave de cifrado aleatoria que se utiliza para cifrar los datos en la partición. La clave de cifrado se cifra utilizando una clave de cifrado maestra que se crea a partir de la contraseña del usuario. La contraseña del usuario se utiliza para cifrar la clave de cifrado maestra. La clave de cifrado maestra se almacena en la partición y se utiliza para descifrar la clave de cifrado de la partición durante el arranque del sistema. Una vez que la partición se ha descifrado, se puede acceder a los datos en la partición como si no estuvieran cifrados.

LUKS también utiliza el cifrado asimétrico para proporcionar una clave de recuperación. La clave de recuperación se genera como una clave pública durante la creación de la partición LUKS. La clave privada correspondiente se cifra y se almacena en un lugar seguro. En caso de que el usuario olvide la contraseña, la clave de recuperación puede utilizarse para descifrar la clave de cifrado maestra y permitir el acceso a los datos en la partición cifrada. LUKS se utiliza ampliamente en sistemas operativos basados en Linux, como Ubuntu, Fedora y Debian. Es una opción popular para la protección de datos en sistemas Linux debido a su alta seguridad y facilidad de uso.

6. ALGORITMO RSA

El nombre RSA proviene de las iniciales de sus tres creadores, Rivest, Shamir y Adleman, en el año de 1997.Este algoritmo se basa en dos problemas matemáticos: el problema de factorizar números grandes y el problema RSA.

El problema del RSA se define como la tarea de tomar raíces eth módulo a componer n: recuperando un valor m tal que me=c mod n, donde (e, n) es una clave pública RSA y c es el texto cifrado con RSA. Actualmente la aproximación para solventar el problema del RSA es el factor del módulo n. Con la capacidad para recuperar factores primos, un atacante puede computar el exponente secreto d desde una clave pública (e, n), entonces descifra c usando el procedimiento standard. Para conseguir esto, un atacante factoriza n en p y q, y computa (p-1)(q-1) con lo que le permite determinar d y e. No se ha encontrado ningún método en tiempo polinómico para la factorización de enteros largos.

Este algoritmo se usa a menudo en combinación con otros esquemas de cifrado o para firmas digitales que pueden probar la autenticidad e integridad de un mensaje. Por lo general, no se usa para cifrar mensajes o archivos completos, porque es menos eficiente y consume más recursos que el cifrado de clave simétrica. El cifrado RSA se puede utilizar en varios sistemas diferentes. Se puede implementar en OpenSSL, wolfCrypt, cryptlib y otras bibliotecas criptográficas.

7. REFERENCIAS

1. Thakor, V. A., Razzaque, M. A., Darji, A. D., Patel, A. R. (2023). A novel 5-bit S-box design for

lightweight cryptography algorithms. Journal of Information Security and Applications, 73, 103444. https://doi.org/10.1016/j.jisa.2023.103444
2. Fundamentos del cifrado Un repaso a la historia y la evolución de los algoritmos criptográficos y el descifrado. (2018). Digicert. Retrieved March 16, 2023, from https://www.digicert.com/resources/history-of-ciphers-understanding-encryption-whitepaper-es-2019.pdf
3. Conceptos claves en cifrado. (n.d.-b). Surveillance Self-Defense. https://ssd.eff.org/es/module/conceptos-claves-en-cifrado
4. Cifrado AES y RSA. (n.d.-b).https://www.boxcryptor.com/es/encryption/
5. Wolf, G. (n.d.). Criptografía y Seguridad: Bibliotecas y prácticas. SG Buzz. Retrieved March 15, 2023, from https://sg.com.mx/revista/45/criptografia-y-seguridad-bibliotecas-y-practicas
6. C. (2020, March 26). ¿Qué son algoritmos de cifrado? Tipos y características. Ciberseguridad. https://ciberseguridad.com/servicios/algoritmos-cifrado/
7. C. (2022, March 8). ¿Qué es el cifrado RSA y cómo funciona? Ciberseguridad. https://ciberseguridad.com/guias/prevencion-proteccion/criptografia/cifrado-rsa/
8. UPM. (2016, October 7). Píldora formativa 39: ¿Cómo funciona el algoritmo RSA? [Video]. YouTube. https://www.youtube.com/watch?v=CMe0COxZxb0
9. UPM. (2015b, November 2). Píldora formativa 30: ¿Cómo se cifra con el algoritmo AES? [Video]. YouTube. https://www.youtube.com/watch?v=tzj1RoqRnv0
10. Harmening, J. T. (2017b). Virtual Private Networks. Computer and Information Security Handbook. https://doi.org/10.1016/b978-0-12-803843-7.00058-2