Criptografía – El aliado silencioso en la protección de la información.

Ing. Guillermo Mora Granados
Estudiante
Maestría Profesional en Ciberseguridad
Universidad Internacional San Isidro Labrador
San José, Costa Rica
moragranadosguillermo@gmail.com

Resumen – En este artículo se explora la evolución y la importancia de la criptografía en la seguridad de la información en la era digital. Se abordan técnicas de encriptación, desde métodos primitivos hasta algoritmos avanzados como AES-256-CBC y ChaCha20, que se utilizan para proteger datos sensibles en diversas aplicaciones, incluyendo comunicaciones seguras y almacenamiento de información. Se destaca la relevancia de la criptografía en la protección de datos en entornos inseguros, como redes Wi-Fi públicas, y su papel crucial en la autenticación y confidencialidad de contraseñas y transacciones financieras. Al final se muestra una sugerencia de utilización de AES-256-CBC y ChaCha20 combinados en un algoritmo de encriptación de doble capa con un amplio rango de utilización.

Palabras clave – encriptación, aes-256-cbc, chacha20, encriptación asimétrica, encriptación simétrica

Abstract – This article explores the evolution and importance of cryptography in information security in the digital age. It discusses encryption techniques, from primitive methods to advanced algorithms such as AES-256-CBC and ChaCha20, which are used to protect sensitive data in various applications, including secure communications and information storage. The relevance of cryptography in protecting data in insecure environments, such as public Wi-Fi networks, and its crucial role in the authentication and confidentiality of passwords and financial transactions is highlighted. At the end, a suggested use of AES-256-CBC and ChaCha20 combined in a dual-layer encryption algorithm with a wide range of use is shown.

Keywords - encryption, aes-256-cbc, aes-256-cbc, chacha20, asymmetric encryption, symmetric encryption

I. INTRODUCCIÓN

La criptografía es una disciplina fundamental en la protección de la información, que se ha desarrollado a lo largo de los siglos.

Desde técnicas simples utilizadas en la antigüedad hasta los sofisticados algoritmos matemáticos actuales, la criptografía permite el encriptamiento y ocultamiento de datos, asegurando que solo las partes autorizadas puedan acceder a la información sensible.

En un mundo donde las comunicaciones digitales son omnipresentes, la criptografía se convierte en una herramienta esencial para salvaguardar la privacidad y la integridad de los datos, especialmente en un contexto donde las amenazas cibernéticas son cada vez más comunes.

En este artículo, abordaremos una contextualización donde explicaremos conceptos básicos de la criptografía, un poco de historia, a abordaje ligero de algunos de los algoritmos matemáticos utilizados en la actualidad y se muestra un ejemplo práctico de utilización de algoritmos como AES-256-CBC y ChaCha20 para producir cadenas encriptadas prácticamente indescifrables.

II. CONTEXTUALIZACIÓN

La criptografía es la ciencia que estudia las formas de codificación de la información a través de encriptamiento y/u ocultamiento de la misma, con el fin de que nadie sin autorización tengo acceso al mensaje que se desea transmitir o bien, mantener guardado de forma secreto en archivos, o bases de datos.

Esta práctica, no es nueva, se remonta a siglos anteriores. Se tienen registros que los hebreos ya realizaba de forma primitiva encriptamiento de mensajes emplando técnicas muy sencillas pero efectivas como el Atbash que consistía en cambiar la primera letra del abecedario por la última, la segunda por la penúltima y así sucesivamente, este método por sustitución, podría considererase como uno de los primeros algoritmos de encriptación conocidos.

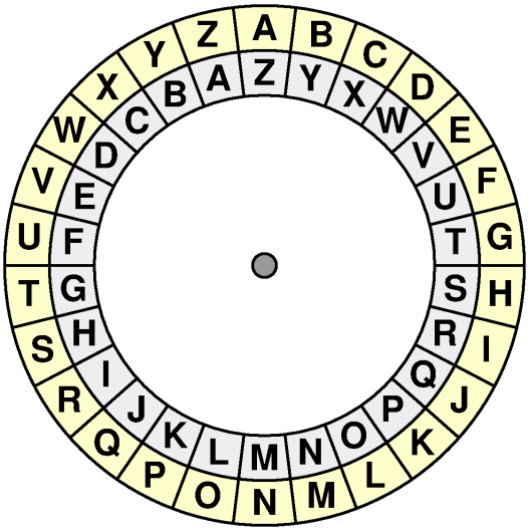


Imagen 1. Cifrado de Atbash

Con el tiempo, la criptografía ha venido mejorando significativamente, llegando a emplear complejos algoritmos matemáticos, mismos que hasta el momento (en el que la computación cuántica no ha sido ampliamente utilizada) y con la capacidad de computación actual, son prácticamente irrompibles.

III. LA CRIPTOGRAFÍA

El esquema básico de encriptamiento es relativamente sencillo.

Primeramente se tiene un texto llamado plain text (o texto claro), éste se somete a un proceso de cifrado (ocultamiento o encriptamiento) mediante la aplicación de un algoritmo, dejando dicho texto ininteligible y generándose además una clave que permita desencriptarlo. Una vez codificado, puede almacenarse o enviarse a algún destinatario sin que exista la posibilidad de ser visualizado y hacer mal uso de su contenido a menos que se conozca y/o se tenga acceso a la llave correspondiente o aplique algún método de criptoanálisis (descifrar código sin el uso del algoritmo original) siendo esto último, trabajo de personas altamente especializadas en seguridad y encriptamiento de datos.

La aplicación de la criptografía es variada y muy útil. La mayoría de las transacciones comerciales y financieras a través de internet (pago de servicios, adquisición de bienes, renta de vehículos, suscripciones, operaciones bancarias como transacciones, compras por internet, entre otras), deben cifrar la información considerada como sensible (número de cuenta, tarjetas de crédito o datos personales) antes de ser enviada por algún medio de comunicación. Una vez recibida, se desencripta haciendo uso de una llave y se obtiene el texto original.

La razón por la que debe ser cifrada, es debido a que dichos medios pueden ser altamente inseguros (como las redes Wi Fi

públicas), existiendo alrededor de ellos infinidad de intrusos o sniffers (virus de computadoras que interceptan la información que se transmite entre los distintos dispositivos a trvaés de internet).

Sin embargo, encriptar datos no es exclusivo de las comunicaciones, también existen programas que cifran información sensible para el usuario o la organización (documentos, bases de datos e incluso imágenes) y que debe ser almacenada aplicando medidas de seguridad extremas evitando que la información pueda ser leída en caso de caer en manos de usuarios indeseables.

Otra aplicación de la criptografía es en las contraseñas. Normalmente, las passwords de los usuarios, antes de ser almacenadas en su perfil, se encriptan utilizando algoritmos especiales, de tal forma que ni el mismo administrador del sistema operativo sea capaz de visualizarlas, logrando con ello garantizar su confidencialidad.

TIPOS DE ENCRIPTAMIENTO

Con respecto a los tipos de algoritmo de encriptamiento, existe una infinidad de los ellos, unos más seguros que otros, sin embargo, si tuviéramos que agruparlos de alguna manera, tendríamos dos grandes categorías como son:

Encriptado Simétrico

Consiste en un algoritmo de encriptación/desencriptación, que utiliza una sola clave para ambas operaciones.

Implementar la criptografía simétrica, especialmente con hardware, puede ser muy eficaz porque no experimenta ningún retraso de tiempo significativo como resultado del cifrado y descifrado.

La criptografía simétrica, también, proporciona un grado de autenticación porque los datos cifrados con una clave simétrica no se pueden descifrar con ninguna otra.

Por lo tanto, siempre que las dos partes que la utilicen para cifrar las comunicaciones mantengan en secreto la clave simétrica, cada una de las partes puede estar segura de que se está comunicando con la otra siempre que los mensajes descifrados sigan teniendo sentido.

Normalmente, una clave simétrica se puede intercambiar con otro participante de confianza, pues, por lo general, produce una clave única para cada par de participantes.

Puede estar seguro de que cualquier mensaje que intercambie, que esté encriptado en una clave específica, sólo podrá ser descifrado por el otro participante que tenga la misma clave; de esta forma, la clave debe mantenerse en secreto para cada participante.

En consecuencia, estas claves también se denominan cifrados de clave secreta. Si alguien más encuentra la clave, afectará tanto a la confidencialidad como a la autenticación.

Una persona con una clave simétrica no autorizada no solo puede descifrar los mensajes enviados con esa clave, sino que, también, puede cifrar los mensajes nuevos y enviarlos como si procedieran de una de las dos partes que originalmente usaban la clave.

Encriptado Asimétrico

La criptografía asimétrica, también conocida como criptografía de clave

pública, es un proceso que utiliza un par de claves relacionadas, una clave pública y otra privada, para cifrar y descifrar un mensaje, y protegerlo de accesos o usos no autorizados.

Una clave pública es una clave criptográfica que puede ser utilizada por cualquier persona para cifrar un mensaje de manera que sólo pueda ser descifrado por el destinatario con su clave privada.

Una clave privada -también conocida como clave secreta- sólo se comparte con el iniciador de la clave.

Cuando alguien quiere enviar un mensaje cifrado, puede obtener la clave pública del destinatario de un directorio público y utilizarla para cifrar el mensaje antes de enviarlo.

El destinatario del mensaje puede entonces descifrarlo utilizando su clave privada correspondiente. Si el remitente encripta el mensaje con su clave privada, sólo podrá desencriptarlo con la clave pública del remitente, lo que permitirá autentificarlo.

Estos procesos de cifrado y descifrado se producen automáticamente pues los usuarios no necesitan bloquear y desbloquear físicamente el mensaje.

El principal beneficio de la criptografía asimétrica es el aumento de la seguridad de los datos. Es el proceso de cifrado más seguro porque los usuarios nunca tienen que revelar o compartir sus claves privadas, lo que disminuye las posibilidades de que un ciberdelincuente descubra la clave privada de un usuario durante la transmisión.

Es importante mencionar, que este método es ínfimamente más lento que el asimétrico, sin embargo, su aumento en el tiempo de ejecución, es prácticamente imperceptible en condiciones normales.

IV. LA MATEMÁTICA DETRÁS DE LA CRIPTOGRAFÍA

Las técnicas actuales de encriptamiento son sofisticadas y se ayudan de teorías y conceptos matemáticos como la teoría de la información, teoría de números, algebra abstracta, aritmética modular, geometría algebraica, curvas elípticas, entre otras más.

En álgebra abstracta, los elementos combinados por diversas operaciones generalmente no son interpretables como números, razón por la cual el álgebra abstracta no puede ser considerada una simple extensión de la aritmética. El estudio del álgebra abstracta ha permitido observar con claridad lo intrínseco de las afirmaciones lógicas en las que se basan todas la matemática y las ciencias naturales, y se usa hoy en día prácticamente en todas las ramas de la matemática.

La aritmética modular, es un conjunto de métodos que permiten la resolución de problemas sobre números enteros.

Un uso familiar de la aritmética modular es en el reloj de 12 horas, en el que el día se divide en dos períodos de 12 horas. Si la hora es a las 7:00, entonces 8 horas más tarde serán las 3:00. La adición simple daría como resultado 7 + 8 = 15, pero a las 15:00 se lee como 3:00 en la esfera del reloj porque los relojes "se envuelven" cada 12 horas y el número de hora comienza de nuevo en cero cuando llega a las 12.

La criptografía de curva elíptica (ECC, por sus siglas en inglés) es una forma de criptografía de clave pública que se basa

en las matemáticas de las curvas elípticas. Ofrece una forma segura de realizar operaciones criptográficas, como el intercambio de claves, las firmas digitales y el cifrado. La ECC es una alternativa al cifrado de Rivest-Shamir-Adleman (RSA), que se lanzó por primera vez en 1977.

V. SHA-256-CBC

AES-256-CBC es un algoritmo de cifrado que utiliza el estándar de cifrado simétrico AES con una clave de 256 bits, lo que ofrece un alto nivel de seguridad.

En el modo CBC (Cipher Block Chaining), el mensaje se divide en bloques de 128 bits, y cada bloque de texto claro se combina con el bloque cifrado anterior (o un vector de inicialización, IV, en el caso del primer bloque) utilizando una operación XOR antes de ser cifrado con AES.

Este proceso asegura que el cifrado de cada bloque depende de los bloques anteriores, lo que proporciona una mayor seguridad al cifrado.

El IV debe ser único y aleatorio para cada operación de cifrado para garantizar que el mismo texto claro no produzca el mismo texto cifrado en diferentes ocasiones.

Para descifrar, se realiza el proceso inverso: el texto cifrado se divide en bloques, se descifra cada bloque usando AES-256, y luego se combina con el bloque cifrado anterior usando XOR para recuperar el texto claro original.

VI. CHACHA20

ChaCha20 es un algoritmo de cifrado de flujo que utiliza una clave de 256 bits para proporcionar un alto nivel de seguridad.

A diferencia de los algoritmos de cifrado en bloque como AES, ChaCha20 cifra los datos en flujo, es decir, procesa el texto claro en un flujo continuo en lugar de en bloques.

El funcionamiento de ChaCha20 se basa en una secuencia de números pseudoaleatorios generada por un "estado" interno que incluye la clave de 256 bits, un contador de 64 bits y un nonce (número único usado una sola vez) de 64 bits. La clave y el nonce se combinan con el contador para inicializar el estado interno. A medida que se cifra el texto claro, el algoritmo genera un flujo de clave pseudoaleatorio que se combina con el texto claro mediante una operación XOR para producir el texto cifrado.

El mismo flujo de clave se utiliza para descifrar los datos: el texto cifrado se combina con el flujo de clave mediante una operación XOR para recuperar el texto claro original. La combinación de la clave, el nonce y el contador asegura que el flujo de clave generado es único para cada operación de cifrado, proporcionando así una fuerte protección contra ataques.

La simplicidad y eficiencia de ChaCha20 lo hacen adecuado para aplicaciones que requieren alta velocidad y seguridad, como en comunicaciones seguras y almacenamiento de datos.

VII. APLICACIÓN PRÁCTICA

cryIN – cryOUT / PHP

El autor de este artículo ha desarrollado un conjunto de funciones utilizando el lenguaje de programación PHP. Estas funciones son cryIN, la cual se utiliza para encriptar datos, la función cryOUT, la cual se utiliza para desencriptar los datos

previamente encriptados por cryIN, y tres funciones auxiliares que se encargan de revisar si existe (y crear en caso de no existir) el archivo clave necesario para el proceso de descriptación.

En esta implementación, se utiliza una combinación de algoritmos de cifrado para proporcionar una capa adicional de seguridad en el proceso de encriptación y desencriptación de datos. Se integra tanto AES-256-CBC como ChaCha20 para garantizar una protección robusta de la información.

El proceso de encriptación comienza verificando la existencia de una clave para el algoritmo ChaCha20. Si esta clave no se encuentra en una ubicación segura del servidor, se genera una nueva clave. Esta clave se utiliza junto con una contraseña compartida en ambas funciones de encriptación (cryIN para cifrar y cryOUT para descifrar).

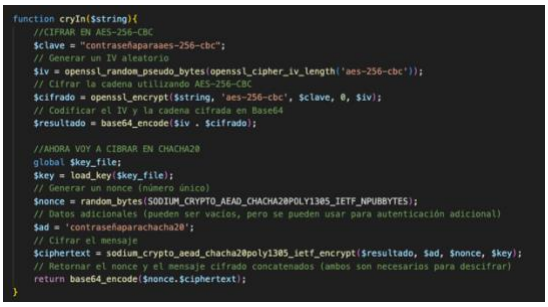
```php
// Función para guardar la clave en un archivo
function save_key($key, $filepath){
    file_put_contents($filepath, $key);
}

// Función para cargar la clave de un archivo
function load_key($filepath){
    return file_get_contents($filepath);
}

// Generar una clave segura solo si el archivo no existe
if (!file_exists($key_file)){
    $key = sodium_crypto_aead_chacha20poly1305_ietf_keygen();
    save_key($key, $key_file);
}
```

Imagen 2. Funciones auxiliares para archivo .key

En la función de encriptación cryIN, se recibe el texto plano, que primero se cifra utilizando AES-256-CBC. El resultado cifrado con AES se pasa entonces a través del algoritmo ChaCha20 para una segunda capa de cifrado. Finalmente, el texto cifrado resultante se codifica en base64 para su transmisión o almacenamiento.



```php
function cryIn($string){
    //CIFRAR EN AES-256-CBC
    $clave = "contraseñaparaaes-256-cbc";
    // Generar un IV aleatorio
    $iv = openssl_random_pseudo_bytes(openssl_cipher_iv_length('aes-256-cbc'));
    // Cifrar la cadena utilizando AES-256-CBC
    $cifrado = openssl_encrypt($string, 'aes-256-cbc', $clave, 0, $iv);
    // Codificar el IV y la cadena cifrada en Base64
    $resultado = base64_encode($iv . $cifrado);

    //AHORA VOY A CIBRAR EN CHACHA20
    global $key_file;
    $key = load_key($key_file);
    // Generar un nonce (número único)
    $nonce = random_bytes(SODIUM_CRYPTO_AEAD_CHACHA20POLY1305_IETF_NPUBBYTES);
    // Datos adicionales (pueden ser vacíos, pero se pueden usar para autenticación adicional)
    $ad = 'contraseñaparachacha20';
    // Cifrar el mensaje
    $ciphertext = sodium_crypto_aead_chacha20poly1305_ietf_encrypt($resultado, $ad, $nonce, $key);
    // Retornar el nonce y el mensaje cifrado concatenados (ambos son necesarios para descifrar)
    return base64_encode($nonce.$ciphertext);
}
```

Imagen 3. Función cryIN

Por otro lado, la función de descifrado cryOUT realiza el proceso inverso. Toma el texto cifrado codificado en base64 como entrada y lo decodifica. Luego, se descifra el texto utilizando ChaCha20, recuperando el resultado cifrado con AES. Finalmente, se aplica la desencriptación con AES-256-CBC para obtener el texto plano original.

```php
function cryOut($cadenaCifrada){
    //DESCIFRAR EL CHACHA20
    global $key_file;
    $key = load_key($key_file);
    // Decodificar el mensaje base64
    $ciphertext = base64_decode($cadenaCifrada);
    // Extraer el nonce y el mensaje cifrado
    $nonce = mb_substr($ciphertext, 0, SODIUM_CRYPTO_AEAD_CHACHA20POLY1305_IETF_NPUBBYTES, '8bit');
    $ciphertext = mb_substr($ciphertext, SODIUM_CRYPTO_AEAD_CHACHA20POLY1305_IETF_NPUBBYTES, null, '8bit');
    // Datos adicionales (deben coincidir con los utilizados para cifrar)
    $ad = 'contraseñaparachacha20';
    // Descifrar el mensaje
    $cadenaCifrada = sodium_crypto_aead_chacha20poly1305_ietf_decrypt($ciphertext, $ad, $nonce, $key);

    // DESCIFRAR EL AES-256CBC
    //$cadenaCifrada = substr($cadenaCifrada, strpos($cadenaCifrada, "?") + 1);
    $clave = "contraseñaparaaes-256-cbc";
    // Decodificar la cadena Base64
    $cadenaDecodificada = base64_decode($cadenaCifrada);
    // Obtener el IV de la cadena decodificada
    $longitudIV = openssl_cipher_iv_length('aes-256-cbc');
    $iv = substr($cadenaDecodificada, 0, $longitudIV);
    // Obtener la cadena cifrada
    $cifrado = substr($cadenaDecodificada, $longitudIV);
    // Descifrar la cadena utilizando AES-256-CBC
    $descifrado = openssl_decrypt($cifrado, 'aes-256-cbc', $clave, 0, $iv);
```

Imagen 4. Función cryOUT

Este enfoque de cifrado en doble capa proporciona una mayor seguridad al combinar las fortalezas de ambos algoritmos de cifrado. AES-256-CBC asegura una sólida protección con un cifrado en bloque, mientras que ChaCha20 añade una capa adicional de seguridad a través del cifrado en flujo, aumentando así la resistencia del sistema contra posibles ataques.

Es importante mencionar, que las aplicaciones de estas funciones son amplias y variadas, desde encriptar contraseñas, cadenas de texto de variables GET en PHP, o bien, para encriptar

contenido delicado y sensible a nivel de base de datos.

XIII. CONCLUSIONES

La criptografía se erige como un pilar fundamental en la seguridad de la información en la actualidad.

La combinación de algoritmos de encriptación robustos, como AES-256-CBC y ChaCha20, proporciona una defensa eficaz contra posibles ataques y garantiza la confidencialidad de los datos.

A medida que la tecnología avanza y surgen nuevas amenazas, la criptografía seguirá evolucionando, adaptándose a los desafíos del futuro y asegurando que la información sensible permanezca protegida.

La comprensión y aplicación de estas técnicas son vitales para cualquier individuo o entidad que busque resguardar su información en un entorno digital cada vez más complejo.

REFERENCIAS

Hernández Encinas, L. (2016). La criptografía: (ed.). Editorial CSIC Consejo Superior de Investigaciones Científicas. https://elibro.net/es/lc/uisil/titulos/41843

Fraleigh, John B.: *Álgebra abstracta* (1987).

Carmona Collado, Luis Miguel. «Congruencias» (HTML). Introducción a la aritmética entera y modular. Universidad politécnica de Madrid. Consultado el 11 de agosto de 2024.

Trevino, Aranza. «¿Qué es la criptografía de curva elíptica?» *Keeper Security* (blog), 2023. https://www.keepersecurity.com/blog/es/2023/06/07/what-is-elliptic-curve-cryptography/#:~:text=La%20criptograf%C3%ADa%20de%20curva%20el%C3%ADptica%20(ECC%2C%20por%20sus%20siglas%20en,firmas%20digitales%20y%20el%20cifrado.