

Fundamentos sobre Criptografía

Jorge Alejandro Mieres
jamieres@gmail.com

Nota 2 de 5

El creciente desarrollo de los canales de comunicación utilizados para la transmisión de información de todo tipo, obliga a la implementación de nuevas herramientas y mecanismos que permitan garantizar un adecuado grado de seguridad sobre los datos que transitan a través de los diferentes canales de comunicación.

El objetivo del presente documento es brindar los conocimientos básicos sobre cuál es el origen de la criptografía, cuáles son los algoritmos más utilizados, y de qué manera interactúan cotidianamente en las vidas de las personas para garantizar, sin que ello se perciba, el grado necesario de seguridad.

Garantizar comunicaciones seguras y confiables no es una tarea sencilla, sobre todo teniendo en cuenta que día a día surgen nuevas metodologías y técnicas de ataques dirigidos que atentan contra los sistemas informáticos con el objetivo de obtener información sensible y confidencial de los usuarios.

Seguridad de la Información

- 1.- Fundamentos sobre Seguridad de la Información.
- 2.- Fundamentos sobre Criptografía.**
- 3.- Principios básicos sobre el protocolo TCP/IP.
- 4.- Políticas de Seguridad de la Información.
- 5.- Amenazas informáticas.

Paralelamente a ello, en la vida cotidiana, cada vez que una persona ingresa a su Home Banking, cuando utiliza el cajero automático para realizar transacciones, cuando utiliza el teléfono celular o cuando simplemente accede a la computadora a través de un proceso de autenticación (usuario y contraseña),

en forma totalmente transparente y sin percibirlo, está haciendo uso de diferentes sistemas que involucran procedimientos y sistemas criptográficos.

En este aspecto, implementar mecanismos que permitan ocultar la información se ha convertido en una necesidad innegable e inmutable de los sistemas de seguridad, siendo prácticamente imposible encontrar en la actualidad un sistema informatizado que no utilice algún sistema de protección, constituyendo una herramienta fundamental y decisiva para las implementaciones de de protección que operan por canales vulnerables.

Introducción a la criptografía

Etimológicamente hablando, la palabra criptografía tiene su origen en el término griego "*Kriptos*" (oculto) y "*Grafos*" (escritura), por lo que su significado se constituye en "*escribir de un modo secreto o enigmático*".

Antiguamente, la criptografía era considerada un arte, y de hecho mucha bibliografía se refiere a ella bajo ese concepto; sin embargo, en la actualidad esta conceptuada como una ciencia, donde el objetivo que busca es transformar un texto perfectamente legible, denominado texto claro, en un texto totalmente ilegible, denominado texto cifrado o criptograma, utilizando una serie de métodos y técnicas que se conocen como algoritmos.

Una definición más técnica es "*...rama inicial de las Matemáticas y en la actualidad de la Informática y la Telemática, que hace uso de técnicas y métodos con el objeto principal de cifrar un mensaje o archivo por medio de un algoritmo, usando una o varias claves.*"

El proceso que modifica la información recibe el nombre de cifrado, siendo su proceso inverso conocido bajo el término de descifrado, permitiendo a los usuarios autorizados poder reestablecer el texto ininteligible a su estado original; es decir, el texto claro inicialmente cifrado.

En resumidas palabras, el objetivo de la ciencia criptográfica es proteger la información que se envía a través de canales potencialmente inseguros utilizando diferentes técnicas de cifrado de manera que el mensaje o el archivo pueda ser compartido con las personas a las cuales vaya dirigido el mensaje.

Asimismo, con el fin de brindar protección, la criptografía aplica a la información códigos y funciones matemáticas denominados algoritmos de cifrado/descifrado; la técnica que se ocupa de "romper" esos algoritmos se llama criptoanálisis.

El conjunto formado por la criptografía y el criptoanálisis conforman lo que se conoce como criptología, que está relacionada, a su vez, con disciplinas científicas como la "Teoría de la información", "Teoremas de la matemática discreta", "Estadística y probabilidad", entre otras.

En seguridad de la Información, la ciencia criptográfica posee una importancia relevante ya que a través de ella se garantiza:

- **Autenticación:** permite asegurar que el mensaje fue enviado realmente por quien dice haberlo hecho.
- **Confidencialidad:** asegura que el mensaje podrá ser leído sólo por el destinatario.
- **Integridad:** permite asegurar que el mensaje no fue modificado; es decir, un mensaje es íntegro porque no fue alterado.
- **No repudio de emisor y receptor:** previene que alguna de las partes involucradas niegue haber enviado o recibido un mensaje.

Funcionamiento de un sistema criptográfico

El funcionamiento de los sistemas de cifrado y descifrado dependen de unas claves que actúan como modificador del algoritmo. De esta forma, aunque los algoritmos sean públicos, si no se cuenta con la clave correspondiente para poder descifrar el mensaje resulta muy difícil llevar a cabo con éxito el proceso de descifrado.

Por ello, siempre es recomendable que los algoritmos sean públicos y se encuentren bien documentados, ya que de esta manera podrán ser sometidos a rigurosas y constantes pruebas para determinar su grado de robustez y seguridad.

En la actualidad, la mayoría de los algoritmos criptográficos son públicos, se encuentran bien documentados y sientan sus bases en la ejecución de diferentes operaciones (sustitución, transposición) que se aplican sobre la información que constituye el texto claro; con lo cual los caracteres del texto original se codifican mediante bits y sobre esos bits se realizan operaciones de transposición y sustitución, dependiendo del algoritmo utilizado.

La idea de hacer público y documentar el algoritmo se encuentra basada en el concepto de no caer en aquello que en criptografía y seguridad de la información se conoce como "*seguridad por oscuridad*". Este término se refiere a la práctica de utilizar el secreto (de diseño, de implementación, etc.) para garantizar la seguridad, en este caso, del algoritmo de cifrado.

En términos criptográficos, lo contrario a "*seguridad por oscuridad*" está determinado por el "*principio de Kerckhoff*" donde se establece que la fortaleza de un algoritmo reside exclusivamente en mantener secreta la clave y no en mantener en secreto el algoritmo.

Con relación a las diferentes operaciones que son aplicadas al texto claro, las sustituciones agregan *confusión* al mensaje cifrado de manera que el análisis de patrones estadísticos sea dificultoso. En cambio, las operaciones de transposición provocan *difusión* en la información cifrada logrando disimular las redundancias del texto claro al ocupar todo el criptograma.

Por otra parte, es preciso no confundir los términos "*clave*" del sistema criptográfico que suele referirse a la información generada por una máquina y en un formato no legible y el término "*contraseña*" que es reservado para la secuencia de información establecida por una persona mediante la combinación de caracteres alfanuméricos.

Sistemas criptográficos

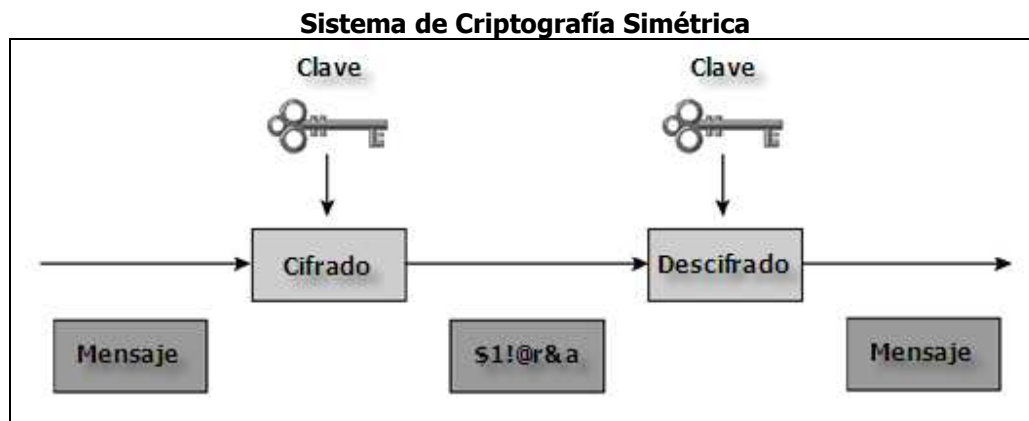
Un sistema criptográfico se encuentra constituido por los algoritmos de cifrado (una transformación del texto que puede ser invertida), los algoritmos de descifrado (el algoritmo inverso) y por la clave que define de forma unívoca el mensaje cifrado o descifrado.

Los sistemas criptográficos más importantes son dos, la criptografía simétrica y la criptografía asimétrica:

Criptografía simétrica

La criptografía simétrica, o criptografía de clave privada, es el método más conocido, involucra una clave única y secreta que es compartida por el emisor y el receptor. De esta manera, la información puede ser cifrada y descifrada a partir de esa clave secreta. En tal sentido, la seguridad de este tipo de sistema criptográfico radica en, precisamente, mantener en secreto la clave.

La característica más apreciada de este tipo de sistemas reside en la velocidad de cifrado y eficiencia desde el punto de vista computacional, ya que se basan en operaciones matemáticas sencillas. Sin embargo, posee una serie de puntos débiles que reducen su eficiencia al momento de gestionar y administrar las claves; además de no poseer firma digital.



Por otra parte, dependiendo del tratamiento que se le aplique a la información, los sistemas simétricos tienen dos formas de funcionamiento:

- **Cifrado por bloque (*block cipher*):** también denominado "*poligráfico*", consiste en aplicar el mismo algoritmo de cifrado a un bloque de información varias veces, utilizando la misma clave. De esta manera es posible combinar operaciones de sustitución y transposición.
- **Cifrado por flujo (*stream cipher*):** también llamado "*cifrado de bit a bit*", este sistema simétrico aplica el algoritmo de cifrado a un elemento de información (carácter o bit) mediante un flujo que constituye la clave, que en teoría es aleatorio y de tamaño superior al del mensaje.

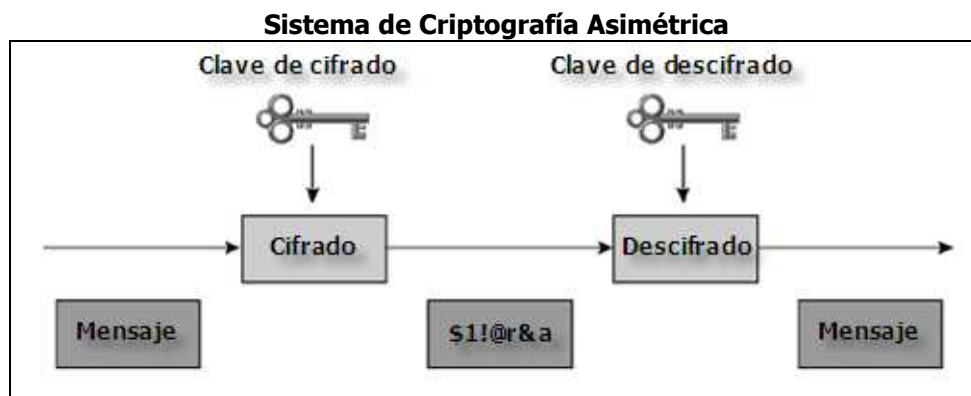
Existen infinitudes de algoritmos que se utilizan en criptografía simétrica, pero los más usados son los siguientes:

- **Data Encryption Standard (DES):** *Estándar de Cifrado de Datos*, este algoritmo es descendiente del criptosistema creado por IBM llamado "*Lucifer*". DES cifra bloques de 64 bits (56 bits de clave y 8 bits de paridad) mediante sustitución. Fue utilizado por el gobierno de Estados Unidos hasta que se determinó que era un algoritmo inseguro.
- **Triple Data Encryption Standard (3DES):** *Triple Estándar de Cifrado de Datos*, utilizando el Standard ANSI X9.52, 3DES es la versión evolucionada de DES, por lo tanto posee compatibilidad con este. Su funcionamiento consiste en cifrar tres veces la información.
- **Advanced Encryption Standard (AES):** *Estándar Avanzado de Cifrado*, también conocido como "*Rijndael*". Algoritmo que resultó ganador en un concurso organizado por el NIST para buscar un algoritmo que sustituyera a DES. AES es un algoritmo de cifrado en bloque que utiliza bloques de 128, 192 o 256 bits y claves de longitud variable de entre 128 y 256 bits.
- **Internacional Data Encryption Algorithm (IDEA):** *Algoritmo Internacional de Cifrado de Datos*, creado en 1990, IDEA trabaja con bloques de texto de 64 bits y utiliza claves de 128 bits. Se destaca por su rapidez y resulta resistente a técnicas de criptoanálisis lineal y diferencial. IDEA es un algoritmo patentado y actualmente tiene problemas de exportación.
- **Twofish:** algoritmo que opera en bloques de 128 bits con clave cuyo tamaño puede alcanzar los 256 bits. Bruce Schneier formó parte del grupo que lo creó. Twofish ocupó el tercer lugar en el concurso organizado por el NIST.

Actualmente, la criptografía simétrica es aplicada en el cifrado de documentos en ofimática, en aplicaciones comerciales de telefonía móvil, en canales de red y en el cifrado de aplicaciones de bases de datos.

Criptografía asimétrica

La criptografía asimétrica, también conocida como criptografía de clave pública, es el método más moderno y a diferencia de la criptografía simétrica, involucra la utilización de dos claves, una clave pública, conocida por todo el mundo y una clave privada conocida sólo por el dueño.



El mecanismo de cifrado consiste en cifrar la información del emisor con la clave que es conocida (clave pública) y descifrarla en el otro extremo, al recibirla, utilizando la otra clave (clave privada).

Es decir, el emisor cifra la información con la clave pública y el receptor la descifra con la clave privada. En este caso, la seguridad del sistema radica en la dificultad computacional de descubrir la clave privada a partir de la clave pública.

Los sistemas criptográficos asimétricos poseen la ventaja de poder intercambiar las claves de manera mucho más fácil, contando además con firma digital. Sin embargo, a pesar de la facilidad, contrariamente a lo sucede con los sistemas simétricos, estos sistemas criptográficos son muy lentos.

Alguno de los algoritmos asimétricos más conocidos son los siguientes:

- ***Diffie-Hellman Key Exchange (Whitfield Diffie – Martin Hellman)***: Diffie-Hellman está basado en algoritmos discretos y fue creado en el año 1976, fue el primer algoritmo asimétrico. En la actualidad, es utilizado para el intercambio de claves a través de medios inseguros.
- ***Rivest-Shamir-Adleman (RSA)***: algoritmo basado en la dificultad de factorizar un número N , producto de dos números primos grandes. Fue creado en el año 1978 y su nombre está formado por los apellidos de los creadores.
- ***Digital Signature Algorithm (DSA)***: *Algoritmo de Firma Digital*, fue publicado en 1991. Como su nombre lo indica, este algoritmo es utilizado para firmar y cifrar información. Una de sus principales desventajas es que requiere mucho más tiempo de procesamiento computacional que el algoritmo RSA.
- ***ElGamal***: algoritmo basado en Diffie-Hellman y escrito durante el año 1985. Este algoritmo es utilizado en el software libre como GNU Privacy Guard (GPG), versiones de Pretty Good Privacy (PGP) y otros sistemas. Su seguridad está directamente relacionada a la capacidad de calcular logaritmos discretos.
- ***Elliptic Curve Cryptosystems (ECC)***: *Criptosistema de Curva Elíptica*, este sistema criptográfico se encuentra basado en las matemáticas de curvas elípticas. Según sus autores, ECC es más rápido y utiliza claves más cortas que otros algoritmos garantizando un nivel de seguridad equivalente.

Ataques criptográficos

Con el fin de comprometer la seguridad de un criptosistema, un atacante (criptoanalista, hacker, etc.) intentará quebrar el algoritmo criptográfico utilizando diferentes técnicas y metodologías que le faciliten la tarea.

En tal sentido, un ataque criptográfico exitoso permitirá obtener el mensaje o la clave con la que la información fue cifrada y, consecuentemente a ello, conseguirá conocer el secreto.

A continuación se mencionan los ataques a los que suelen ser sometidos los criptosistemas:

- **Ataque por fuerza bruta:** consiste en probar todas las claves posibles, es una técnica que consume mucho tiempo.
- **Ataque por diccionario:** consiste en intentar romper el sistema criptográfico a partir de una lista que contiene posibles contraseñas.
- **Analíticos:** se utilizan algoritmos y manipulación de operaciones algebraicas para reducir la complejidad del ataque.
- **Estadísticos:** se basan en las debilidades estadísticas en el diseño del sistema.
- **Implantación:** no se ataca el algoritmo de cifrado o descifrado, se ataca cómo fue implantado.
- **Ciphertext-only attack (COA):** el atacante intenta descifrar directamente el texto cifrado.
- **Known-plaintext attack (KPA):** el atacante intenta descifrar el texto cifrado conociendo parte del texto claro.
- **Chosen-plaintext attack (CPA):** el atacante obtiene el texto cifrado que corresponde a un texto claro conocido.
- **Chosen-ciphertext attack (CCA):** en este caso, el atacante obtiene un texto claro que corresponde a un determinado texto cifrado.

De todas formas, tenga presente que la seguridad de un sistema criptográfico, desde un punto de vista práctico, se basa en la robustez que posee su algoritmo frente a la acción de los diferentes ataques.

Historia de la Criptografía

Los primeros sistemas criptográficos fueron empleados por los griegos y los romanos. Los griegos durante el año 500 a.C., para poder ocultar los mensajes, enrollaban una tira de cuero en un cilindro llamado "*scytale*", de esta forma, al desenrollar el cuero, sólo se apreciaba una lista de letras sin sentido alguno.

Por su parte, en el Imperio Romano, Julio César escribía mensajes cifrados para Cícero y sus Generales utilizando una técnica de cifrado que hoy lleva su nombre, "*Cifrado César*". Esta técnica consistía en un simple método de sustitución donde cada letra del mensaje a ocultar era reemplazada por la letra que se encontraba tres posiciones más adelante en el alfabeto latino.

Posteriormente, una de las primeras técnicas polialfabéticas fue desarrollada por el sabio renacentista Leon Battista Alberti al diseñar discos que poseían el alfabeto grabado, con ellos se conseguía que diferentes letras del texto cifrado representaran a la misma letra del texto claro en diferentes puntos del criptograma.

En el año 1518 un monje llamado Benedictino Trithemius escribió el primer tratado de criptografía que se conoció bajo el nombre de "*Polygraphia*". Años después, entre 1784 y 1789, Thomas Jefferson, del Gobierno Francés, utilizó una "*rueda criptográfica*" para mantener en secreto sus comunicaciones.

Otro algoritmo histórico de sustitución polialfabética fue el conocido como "*cifrado de*

Vigenère”, propuesto por un diplomático francés llamado Blaise de Vigenère en el año 1586. Para realizar el cifrado de la información, este algoritmo se basaba en un “*cuadrado de Vigenère*”. Luego, a mediados del siglo XIX, este sistema fue quebrado.

Un nuevo hecho trascendente se produjo durante la 2da. Guerra Mundial donde los alemanes utilizaban una máquina criptográfica llamada “*Enigma*” para cifrar las comunicaciones entre el centro de mando y las tropas.

Paralelamente a ello, en la ciudad de Bletchley Park, ubicada al Norte de Londres, un grupo de científicos polacos entre los que se encontraba Alan Turing trabajaba en un proyecto que tenía como meta descifrar los mensajes cifrados por los alemanes con la máquina *Enigma*. Este proyecto se conoció como “*ULTRA*”.

De esta manera, fueron viendo la luz máquinas criptográficas cada vez más complejas basadas en técnicas como “*discos rotativos*” como la máquina Enigma que utilizaba tres discos rotativos con una cantidad de claves posibles que ascendía a 1.020. Otras máquinas criptográficas que utilizaban esta técnica son la TYPEX del Reino Unido y la Converter M-209 de Estados Unidos.

Glosario

Algoritmo: función matemática utilizada para cifrar y descifrar.

Confusión: transformación sobre el texto claro que busca mezclar los caracteres que lo constituyen de tal forma que la dependencia funcional entre la clave y el criptograma se dificulte.

Criptoanálisis: técnica más importante de la criptología que estudia la robustez del criptograma.

Criptógrafo: máquina utilizada para cifrar información.

Criptograma: información que ha sido sometida a algún proceso de cifrado.

Criptología: ciencia conformada por la criptografía y el criptoanálisis.

Difusión: transformación sobre el texto claro que busca dispersar las propiedades estadísticas del lenguaje sobre todo el texto cifrado.

Firma digital: herramienta utilizada para autenticar la identidad de un remitente.

Método o técnica: proceso utilizado para cifrar o descifrar utilizando una lógica.

NIST: acrónimo de National Institute of Standards Technology (Instituto Nacional de Estándares y Tecnología). Agencia de la Administración de Tecnología del Departamento de Comercio de los Estados Unidos.

Sustitución: reemplazo de bits, caracteres o bloques de caracteres por un sustituto. Cuando la letra o bit se sustituye por un bloque de caracteres, recibe el nombre de “*sustitución homofónica*”.

Transposición: reemplazo del orden de los bits o caracteres que conforman el texto.

Bibliografía consultada

Enciclopedia de la Seguridad Informática. Álvaro Gómez Vieites. Alfaomega-Ra-ma. 2007

Criptografía. Ing. Pablo A. Anselmo. Revistas NEX-IT Specialist #34, #35 y #36. 2007.

Cryptology Unlocked. Reinhard Wobst. Wiley. 2007

Security Plus. Kirk Hausman, Diane Barrett, Martin Weiss. Que. 2003

Bootcamp CISSP. Buenos Aires. Donald R. Glass. 2003

Applied Cryptography. Bruce Schneier. Wiley. 1996