**Cifrado simétrico y asimétrico**

Anteriormente, aprendiste estos términos:

* **Cifrado o encriptación (encryption):** Proceso de convertir datos de un formato legible a uno codificado.
* **Infraestructura de clave pública (PKI, por sus siglas en inglés):** Marco de cifrado que garantiza la seguridad del intercambio de información en línea.
* **Algoritmo de cifrado (cipher):** Algoritmo que cifra la información.

Toda la información digital debe mantenerse privada, segura y protegida. El cifrado es una de las claves para conseguirlo. Es útil para transformar la información en una forma que los destinatarios no autorizados no puedan comprender. En esta lectura, compararás el cifrado simétrico y el asimétrico y aprenderás sobre algunos algoritmos conocidos para cada uno.

**Tipos de cifrado**

Existen dos tipos principales de cifrado:

* **El cifrado simétrico** consiste en utilizar una única clave secreta para el intercambio de información. Debido a que emplea una sola clave tanto para el cifrado como para el descifrado, el remitente y el receptor deben conocer dicha clave para bloquear o desbloquear el cifrado.
* **El cifrado asimétrico** se basa en el uso de un par de claves: una pública, para cifrar los datos, y una privada, para descifrarlos. La clave privada solo se comparte con los usuarios con acceso autorizado.

**La importancia de la longitud de la clave**

Los cifrados son vulnerables a los ataques de fuerza bruta, que consisten en un proceso de prueba y error para descubrir información privada. Esta táctica es el equivalente digital de probar todas los códigos posibles de una cerradura de combinación, intentando encontrar el correcto. En el cifrado moderno, se considera que las claves más largas son más seguras. Una mayor longitud de clave implica más posibilidades que un atacante debe intentar para desbloquear un cifrado.

Una desventaja de tener claves de cifrado largas es que los tiempos de procesamiento son más lentos. Aunque las claves cortas suelen ser menos seguras, se calculan mucho más rápido. Lograr una comunicación de datos rápida en línea, manteniendo la información segura implica un delicado equilibrio.

**Algoritmos aprobados**

Muchas aplicaciones web utilizan una combinación de cifrado simétrico y asimétrico. De esta manera, equilibran la experiencia de usuario con la protección de la información. Como analista de seguridad, debes conocer cuáles son los algoritmos más utilizados.

**Algoritmos simétricos**

* *Triple DES (3DES)* es conocido como un cifrado por bloques debido a la forma en que convierte el texto simple, también llamado texto plano, en texto cifrado en “bloques”. Sus orígenes se remontan al Data Encryption Standard (DES), que fue desarrollado a principios de la década de 1970. DES fue uno de los primeros algoritmos de cifrado simétrico que generó claves de 64 bits. Un **bit** es la unidad más pequeña de medición de datos en una computadora. Como podrás imaginar, Triple DES genera claves de 192 bits, es decir, tres veces más largas. A pesar de que las claves son más largas, muchas organizaciones están dejando de utilizar Triple DES debido a las limitaciones en la cantidad de datos que se pueden cifrar. Sin embargo, es probable que Triple DES siga utilizándose por motivos de compatibilidad con versiones anteriores.
* *Advanced Encryption Standard (AES)*es uno de los algoritmos simétricos más seguros de la actualidad. AES genera claves de 128, 192 o 256 bits. Se considera que las claves criptográficas de este tamaño están protegidas de ataques de fuerza bruta. Se estima que forzar una clave AES de 128 bits podría llevarle miles de millones de años a una computadora moderna.

**Algoritmos asimétricos**

* *Rivest, Shamir y Adleman (RSA)* debe su nombre a sus tres creadores, quienes lo desarrollaron en el Instituto Tecnológico de Massachusetts (MIT). RSA es uno de los primeros algoritmos de cifrado asimétrico que produce un par de claves pública y privada. Los algoritmos asimétricos, como RSA, generan longitudes de clave aún más largas. Esto se debe, en parte, al hecho de que estas funciones están creando dos claves. Los tamaños de clave RSA son 1024, 2048 o 4096 bits. RSA se utiliza principalmente para proteger datos altamente sensibles.
* *El Algoritmo de Firma Digital (DSA)*es un algoritmo asimétrico estándar que fue introducido por el Instituto Nacional de Estándares y Tecnología (NIST) a principios de la década de 1990. DSA también genera longitudes de clave de 2048 bits. Este algoritmo es ampliamente utilizado en la actualidad como complemento de RSA en infraestructuras de clave pública.

**Generación de claves**

Estos algoritmos deben ser implementados cuando una organización elige proteger sus datos. Una forma de hacerlo es mediante el uso de OpenSSL, que es una herramienta de línea de comandos de código abierto que se puede utilizar para generar claves públicas y privadas. OpenSSL es utilizado habitualmente en computadoras para verificar certificados digitales que se intercambian como parte de la infraestructura de clave pública.

**Nota:** OpenSSL es una opción entre varias herramientas disponibles que pueden generar claves utilizando cualquiera de estos algoritmos comunes.

Aunque muchas empresas utilizaban OpenSSL, ya no se recomienda su uso desde el descubrimiento del [error Heartbleed](https://en.wikipedia.org/wiki/Heartbleed) en 2014.

**Lo oscuro no es seguro**

En el mundo de la criptografía, un cifrado debe demostrar  ser invulnerable antes de afirmar que es seguro. Según el [principio de Kerchoff](https://en.wikipedia.org/wiki/Kerckhoffs%27s_principle), la criptografía debe diseñarse de tal manera que todos los detalles de un algoritmo, excepto la clave privada, puedan conocerse sin perder seguridad. Por ejemplo, puedes acceder a todos los detalles sobre cómo funciona el cifrado AES en línea y aun así sigue siendo invulnerable.

Ocasionalmente, las organizaciones implementan sus propios algoritmos de cifrado personalizados. Ha habido casos en los que estos sistemas criptográficos secretos han sido rápidamente descifrados después de hacerse públicos.

**Consejo profesional:** Un sistema criptográfico *no debe* considerarse seguro si su seguridad se basa en mantener en secreto su funcionamiento.

**El cifrado está en todas partes**

Ambos trabajan en conjunto para la seguridad con la experiencia de usuario.

Por ejemplo, los sitios web suelen emplear el cifrado asimétrico para proteger pequeños bloques de datos que son importantes, como nombres de usuario y contraseñas durante el proceso de inicio de sesión. Una vez que alguien obtiene acceso, el resto de su sesión en el sitio web suele cambiar al cifrado simétrico debido a su mayor rapidez.

Este tipo de encriptación de datos es cada vez más exigido por la ley. Regulaciones como el Estándar de Procesamiento de Información Federal (FIPS 140-3) y el Reglamento General de Protección de Datos (RGPD) establecen cómo se deben recopilar, usar y manejar los datos. Cumplir cualquiera de estas regulaciones es fundamental para demostrar a socios comerciales y gobiernos, que los datos de los clientes se manejan de manera responsable.

**Conclusiones clave**

Conocer los conceptos básicos del cifrado es importante para todos los profesionales de la seguridad. El cifrado simétrico se basa en una única clave secreta para proteger los datos. En cambio, el asimétrico utiliza un par de claves, pública y privada. Sus algoritmos de cifrado crean claves de distinto tamaño. Ambos tipos de cifrado se utilizan para cumplir con las regulaciones y proteger los datos en línea.