Resumen criptografía asimétrica

La criptografía asimétrica es uno de los tipos de criptografía informática y una de las técnicas de criptografía más potentes diseñadas en base al uso de una fórmula matemática muy compleja para crear un par de claves: la clave privada y la clave pública. A través de estas claves se establece un canal de comunicación seguro entre las partes, en el que tanto el emisor como el receptor deben usar criptografía asimétrica con un mismo algoritmo definido, que les permitirá crear un juego de claves único e irrepetible para cada uno.

En ese proceso de comunicación, el emisor y el receptor comparten entre ellos sus claves públicas; estas claves cifrarán posteriormente los mensajes que intercambien entre ellos. Y las claves privadas descifrarán esos mensajes para poder ver su contenido. Este proceso hace imposible que un tercero puede interferir en la comunicación y ver el contenido los mensajes.

Este proceso que suena sencillo, pero que esconde años de investigación y potentes algoritmos, se emplea de manera muy habitual en Internet, un ejemplo de encriptación asimétrica lo encontramos en nuestras comunicaciones por WhatsApp o Telegram o en el acceso a nuestros correos electrónicos.

Inicios de la criptografía asimétrica

Sería en 1977 cuando Ron Rivest, Adi Shamir y Leonard Adleman crearían el algoritmo RSA, el primero algoritmo de criptografía asimétrica público que se convertiría en un estándar de la industria hasta nuestros días, donde la evolución de la tecnología ha permitido seguir desarrollando esta técnica de cifrado asimétrico, con resultados cada vez más potentes y seguros.

¿Cómo funciona la criptografía asimétrica?

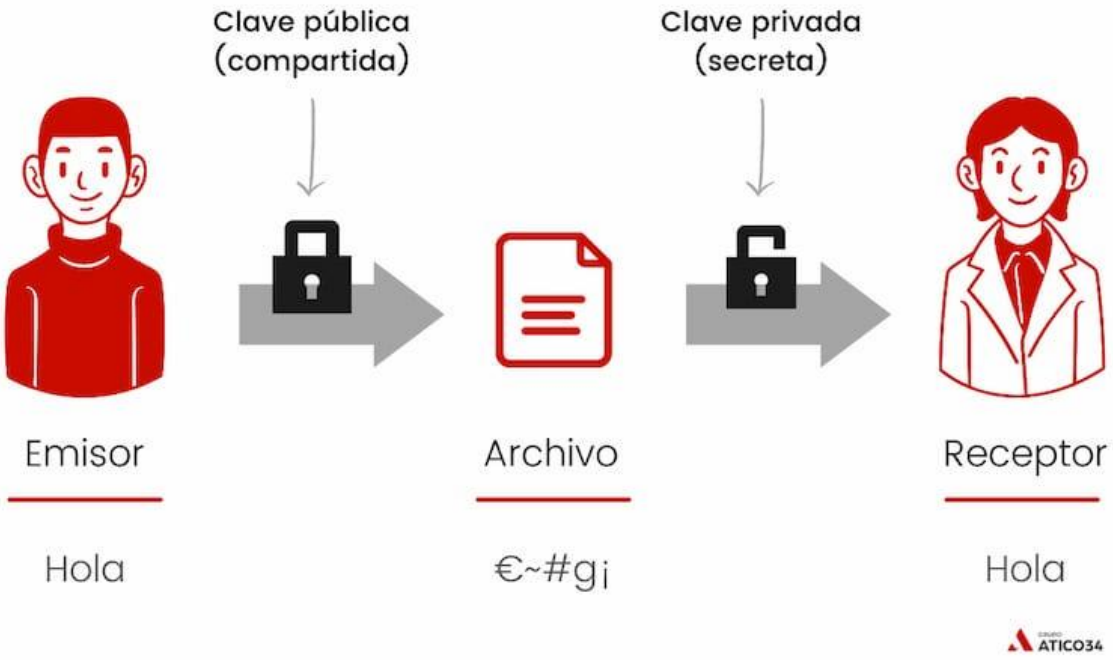
El funcionamiento del cifrado asimétrico sigue una serie de pasos que garantizan que el sistema es completamente seguro y que mantiene el secreto de las comunicaciones que se intercambian a través de él.

Seleccionar el algoritmo y curva de cifrado

El primer paso para que el cifrado asimétrico funcione es escoger el algoritmo que se va a usar, porque cada uno tiene propiedades únicas. Existen en la actualidad decenas de algoritmos, algunos más seguros que otros según su complejidad, pero los más habituales son RSA, ECDSA, EdDSA y ElGamal; cada uno estos algoritmos usa un sistema matemático propio.

Las propiedades de los algoritmos están relacionadas con la curva elíptica que usan para su funcionamiento. Las curvas elípticas consideradas el cifrado asimétrico son numerosas, al menos existen 22 registradas y estudiadas. Por ejemplo, la Curve25519 de Daniel Bernsteins es una de las más utilizadas en algoritmos de cifrado compactos y muy eficientes.

Mientras que en redes blockchain de criptomonedas se usa más la secp256k1.



Generación de claves

Una vez se tienen decidido el algoritmo a usar, el siguiente paso es generar las claves pública y privada.

La primera clave en generarse mediante esta técnica de criptografía es la clave privada. Esta clave solo la poseemos nosotros y surge como el resultado e tomar dato aleatorios y trasladarlos a un problema matemático, del que se obtiene como resultado un número enorme que pasa por un proceso de conversión, para transformarse en una larga cadena de números y letras, que será la clave privada.

Con la clave privada podremos generar la clave pública, a través de un complejo proceso matemático que relaciona la clave privada con una formulación matemática. El resultado vuelve a ser un enorme número que

se transformará en una larga cadena de números y letras que será la clave pública.

Así, la clave privada es una semilla de cifrado, a partir de la cual podemos crear tantas claves públicas como necesitemos. La clave privada nos permite, además, descifrar los mensajes que recibamos de las personas a las que les entregamos nuestras claves públicas. Además, la clave privada nos permite firmar digitalmente los mensajes, dejando así plasmada la autenticidad de la comunicación, puesto que nadie puede duplicar la clave privada.

Por su parte, la clave pública tiene como finalidad que las personas a quien se las damos puedan cifrar los mensajes y enviárnoslos. Es importante señalar que la clave pública permite cifrar mensajes, pero el proceso contrario, descifrarlos, es prácticamente imposible. Esto es así porque la clave privada y la clave pública están relacionadas mediante el algoritmo que se uso para crearlas. La clave pública también verifica la autenticidad de las firmas digitales que llevan nuestros mensajes.

El esquema de envío y recepción de mensajes funciona de la siguiente manera:

1. El usuario A genera un mensaje que es cifrado usando la clave pública del usuario B y firmado por la clave privada de A. Esto garantiza que solo B puede ver este mensaje y corroborar que proviene de A.
2. El mensaje va firmado y cifrado por el canal de comunicación. En caso de ser interceptado, sería inútil tratarlo de leerlo, porque no se podrá descifrar.
3. Cuando el mensaje llega a B, este usuario utilizará su clave privada para descifrarlo, mientras que al mismo tiempo, podrá usar la clave pública de A para validar que el mensaje lo ha enviado realmente A.
4. El proceso se repite al enviar una respuesta.

Gracia a este proceso, la comunicación es segura en canales abiertos, puesto que corromper o manipular el mensaje enviado usando criptografía asimétrica es muy, muy difícil.

Ventajas y Desventajas de la criptografía asimétrica

Entre las ventajas que tiene usar un sistema de criptografía asimétrica encontramos:

- Tiene una alta tasa de seguridad, puesto que el esquema de cifrado es muy complejo; esto hace que el criptoanálisis de estos sistemas sea complicado y que los ataques de fuerza bruta para romperlo resulten inútiles.
- Asegura canales abiertos y públicos de comunicación gracias al empleo de los juegos de claves públicas y privadas.
- Permite autentificar la información gracias un sistema de firma digital. Por ejemplo, en los certificados de la FNMT, se usa un sistema sin repudio cifrado de clave (e0).
- Tienen un alto nivel de confidencialidad e integridad.

Pero la criptografía asimétrica también viene acompañada de algunas desventajas, como por ejemplo:

- Comparado con un cifrado simétrico es computacionalmente más costoso y más lento.
- No es ajeno a problemas externos, por ejemplo, un generador de números aleatorio defectuoso comprometería todo el sistema de cifrado.
- Dada la complejidad de los algoritmos, detectar fallos o bugs es más difícil en este tipo de sistemas.
- Los esquemas de propagación de confianza centralizados pueden suponer una vulnerabilidad ante la manipulación de certificados, si la estructura resulta comprometida.