¿Qué es encriptación Simétrica?

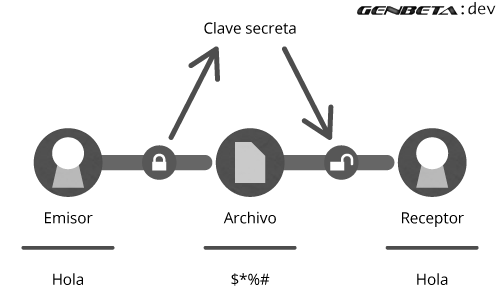
En el **cifrado simétrico** se utiliza la misma clave tanto para el cifrado como para el descifrado de los datos, de tal forma que, si dos interlocutores quieren intercambiar un mensaje secreto, se ha de encontrar la forma de transmitir también la clave de descifrado.

¿Cómo se hace?

Si la clásica criptografía simétrica utiliza el alfabeto para traducir un texto plano en un texto cifrado, el encriptado informático se realiza mediante bits. En este caso se diferencia entre el cifrado de flujo y el de bloque por el algoritmo que utilizan:

* Cifrado en flujo: el cifrado se realiza por bits y se basa en claves muy largas. Cada bit del texto sin formato se correlaciona con un bit en el flujo de claves, de tal forma que se crea un carácter cifrado.
* Cifrado de bloques: en este algoritmo los bits que se han de cifrar se agrupan en bloques de longitud fija, que se corresponden con otros diferentes. Resulta un cifrado de longitud fija.

Imagen:

****

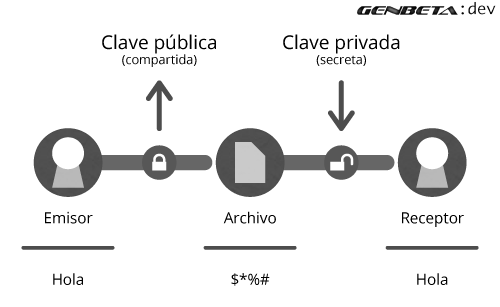
¿Qué es encriptación Asimétrica?

En los **sistemas asimétricos**, por el contrario de la simétrica, cada parte genera su propio par de claves, compuesto de una clave pública (public key) y otra privada (private key).

¿Cómo se hace?

Mientras que en la criptografía simétrica se utiliza la misma clave en ambas partes de la comunicación, en una comunicación cifrada de forma asimétrica ambos interlocutores generan un par de claves en cada lado, de modo que cada uno dispone de **dos claves**, una pública y una privada. Para poder comunicarse de forma encriptada, cada parte ha de dar a conocer su clave pública, lo que suele tener lugar mediante el **servidor de claves**. Es lo que se conoce como **método de clave pública** y privada. La clave privada permanece a buen recaudo y es aquí donde reside la fortaleza de los sistemas criptográficos asimétricos: al contrario que en los simétricos, la clave privada no se conoce.

Imagen:



¿Qué es encriptación hibrida?

Los consisten en la utilización de algoritmos tanto simétricos como asimétricos en la transferencia de datos en Internet. El objetivo de esta combinación es compensar las debilidades de un sistema con las ventajas de otro.

¿Cómo se hace?

Métodos de cifrado simétrico como AES se consideran seguros según el estado actual de la tecnología y permiten procesar también grandes volúmenes de datos de forma rápida y operativamente eficiente. Sin embargo, tal como está diseñado su algoritmo, sobre la base de una clave privada común que se intercambia entre los interlocutores de forma segura, sitúa a los usuarios de los métodos simétricos ante el **problema del intercambio de claves**, únicamente soluble con algoritmos asimétricos. Métodos como el RSA se apoyan en una separación estricta de ambas claves, la privada y la pública, de tal modo que permiten esquivar el problema del intercambio de la clave secreta.