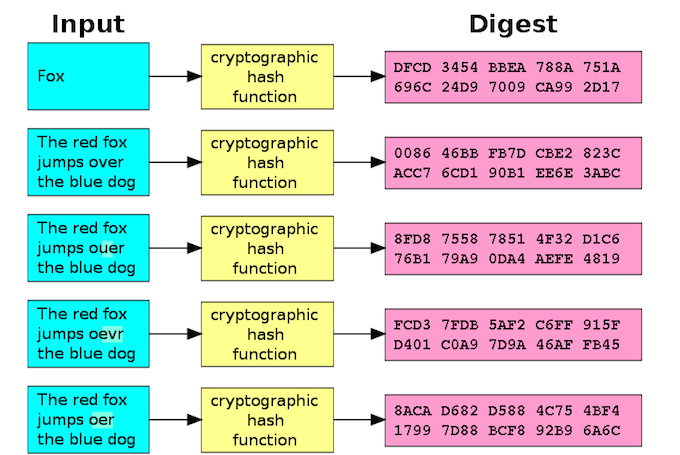
**¿Qué Es Un Hash Y Cómo Funciona?**

Una función criptográfica hash- es un algoritmo matemático que transforma cualquier bloque arbitrario (texto, datos, etc…) en una nueva serie de caracteres con una longitud fija. Independientemente, el valor hash de salida tendrá siempre la misma longitud.



## ****¿Cómo funcionan las firmas digitales?****

Las firmas digitales se basan en la criptografía de clave pública, también conocida como criptografía asimétrica. Normalmente hay tres algoritmos involucrados con el proceso de firma digital:

* **Generación de dos claves que están matemáticamente vinculadas**: un algoritmo proporciona una clave privada junto con su clave pública correspondiente.
* **Firma**: este algoritmo produce una firma al recibir una clave privada y el mensaje que se está firmando.
* **Verificación**: este algoritmo comprueba la autenticidad del mensaje al verificarlo junto con la firma y la clave pública.

Lo primero que debemos conocer si queremos entender qué es una forma digital es el término [***hash***](https://es.wikipedia.org/wiki/Funci%C3%B3n_hash). Los funciones de resumen o *hash*son**algoritmos** que consiguen crear a partir de una entrada (ya sea un texto, una contraseña o un archivo, por ejemplo) una salida alfanumérica de longitud normalmente fija, que representa un **resumen de toda la información** que se le ha dado. Es decir, a partir de los datos de la entrada crea una cadena que solo puede volverse a crear con esos mismos datos.

Para crear una firma digital, el *software* de firma crea un ***hash* unidireccional de los datos electrónicos** que se deben firmar. La clave privada se usa para encriptar el *hash*. El *hash* cifrado junto con otra información es la firma digital.