Criptografía

# Qué es

Es la ciencia de leer y escribir mensajes codificados. Es un componente fundamental en los mecanismos de:

* Autenticación
* Integridad
* Confidencialidad

Definiciones:

* **Autenticación**: Establece la identidad del transmisor y el receptor de la información.
* **Integridad**: Asegura que los datos no han sido alterados.
* **Confidencialidad**: Asegura que nadie, excepto el transmisor y el receptor, son capaces de interpretar los datos transmitidos.
* **Vinculación (antes se llamaba “no repudio”):** Permite vincular un documento o transacción a una persona o un sistema de gestión criptográfico automatizado.

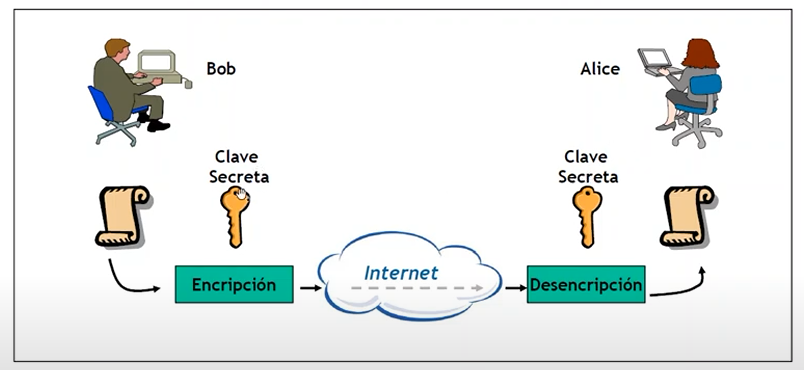
Generalmente un mecanismo criptográfico usa un algoritmo (función matemática) y un valor secreto conocido como clave.

Cuanto más grande es el espacio de claves (rango de valores posibles) más difícil es obtener la clave por medio de ataques de fuerza bruta (probar todas las combinaciones posibles).

# Tipos de encriptado

## Encripción simétrica

Conocida como encripción de “clave secreta” utiliza una clave común y el mismo algoritmo criptográfico para encriptar y desencriptar el mensaje. El punto flojo es la distribución de esta clave (debe ser un canal seguro). Entre 2 es fácil compartir la clave, pero a medida que se escala, es más fácil que se divulgue y deje de ser segura.



Algunos de los algoritmos más conocidos de encripción simétrica son:

* Data encryption standard (DES).
* 3DES (triple DES). Mas difícil de romper por fuerza bruta que DES.
* Rivest Cipher 4 (RC-4).
* International Data Encryption Algorithm (IDEA).
* AES (Advanced Encryption Standard) 128/192/256 (bits).

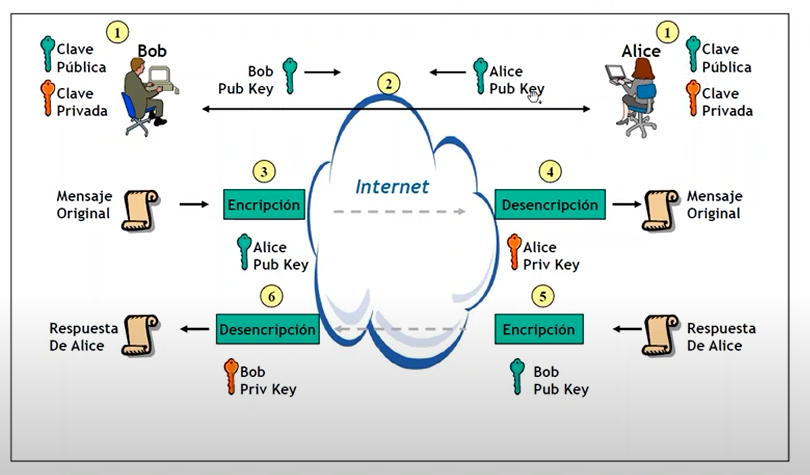
Este mecanismo simétrico no se usa mucho, pero es más eficiente. Sólo se debe saber que existe.

## Encripción Asimétrica

* Conocida como inscripción de “clave pública”.
* Los extremos pueden utilizar el mismo algoritmo o uno diferente pero complementario para encriptar y desencriptar la información.
* Hay dos valores de clave diferentes, pero complementarios, una clave pública y una clave privada.
* Se encripta el mensaje con la clave pública del receptor (conocida o intercambiada libremente), luego el receptor la desencripta usando su propia clave privada.
* La clave privada no se debe divulgar, porque el sistema pierde su valor.

Se usa para: integridad y confidencialidad de datos, no repudio y autenticación del emisor.

### Cómo funciona



Alice quiere mandar mensaje a Bob.

* Alice encripta la clave pública de Bob para enviar el mensaje
* Bob usa su clave privada desencriptar.

Esto garantiza la confidencialidad. Nadie que intercepte puede desencriptarlo.

Cómo garantizar autenticidad y no repudio? Con doble encripción.

* Alice encripta el mensaje con su clave privada y con la pública de Bob.
* Bob desencripta el mensaje con la clave pública de Alice y la pública propia.

### Autenticación y no repudio

Encriptando únicamente con la clave pública del destino no garantizo autentificación ni no repudio, debido a que cualquiera puede hacerlo y no se puede identificar el origen.

Para garantizar autentificación y el no repudio, el emisor encriptara el mensaje con su clave privada, de esta forma el receptor desencriptara el mismo con la clave pública del emisor, de forma tal que se obtiene autentificación y no repudio.

Para garantizar autentificación, no repudio, integridad y confidencialidad primero se encripta el mensaje con la clave privada del emisor y luego con la clave publica del receptor. (doble encriptación para garantizar no repudio 🡪 la clave pública de Alice garantiza confidencialidad, y la privada de Bob me da la certeza de que el mensaje viene de Bob es decir, no repudio – una de las dos encripciones también megarantiza … otra 3ª cosa. )

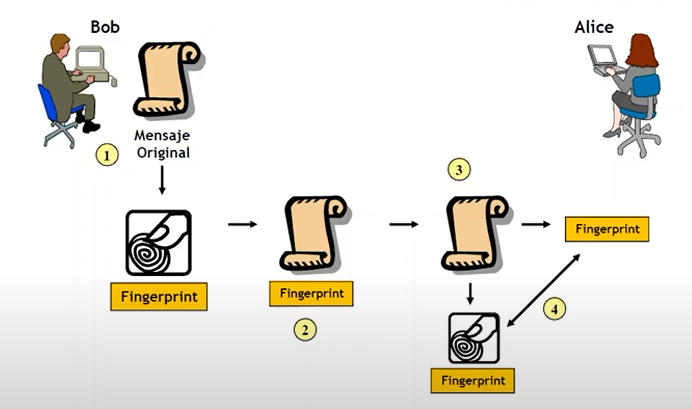
# Funciones de hash

Las funciones Hash garantizan la integridad del mensaje (estándar de la industria).

Una función de Hash toma una entrada de longitud arbitraria y genera una salida de longitud fija. La salida se llama “Digest”.

## Requisitos funciones Hash

* Consistencia: La misma entrada debe generar siempre la misma salida.
* Aleatoriedad: Que impida adivinar el mensaje original.
* Unicidad: Debe ser prácticamente imposible encontrar dos mensajes diferentes que generen el mismo Digest.
* One way: Para un Digest dado, debe ser muy difícil o imposible regenerar el mensaje de entrada.



Bob incluye su cálculo del digesto/fingerprint en el mensaje. Alice lo vuelve a calcular y lo compara con lo enviado. Si coinciden, el mensaje llegó bien.

## Funciones más comunes

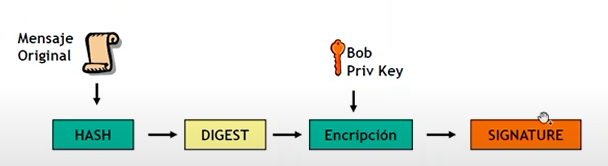
* Message Digest 4 (MD4).
* Message Digest 5 (MD5).
* Secure Hash Algorithm (SHA).

# Firma digital

Una firma digital es un Digest encriptado que se adiciona a un documento. Combina mecanismo de encripción y hash.

Puede utilizarse para:

* Confirmar la identidad del emisor (autenticidad y no repudio).
* Garantizar la integridad del documento.



Se obtiene digesto del mensaje. Ese digesto se encripta con clave privada y se agrega como firma digital. Cualquiera que tenga la clave pública de Bob puede verificar la autenticidad.