Criptografía

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

- Autenticación
- Integridad
- Confidencialidad

Criptografía

Autenticación : Establece la identidad de ambos : el 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

Criptografía

Generalmente un mecanismo criptográfico utiliza un ***algoritmo*** (función matemática) y un valor secreto conocido como "***Clave***"

Cuanto más grande el espacio de claves (rango de posibles valores de la clave) más difícil obtener la clave por medio de ataques por *fuerza bruta*. Los ataques por fuerza bruta consisten en aplicar todas las combinaciones posibles hasta encontrar la clave

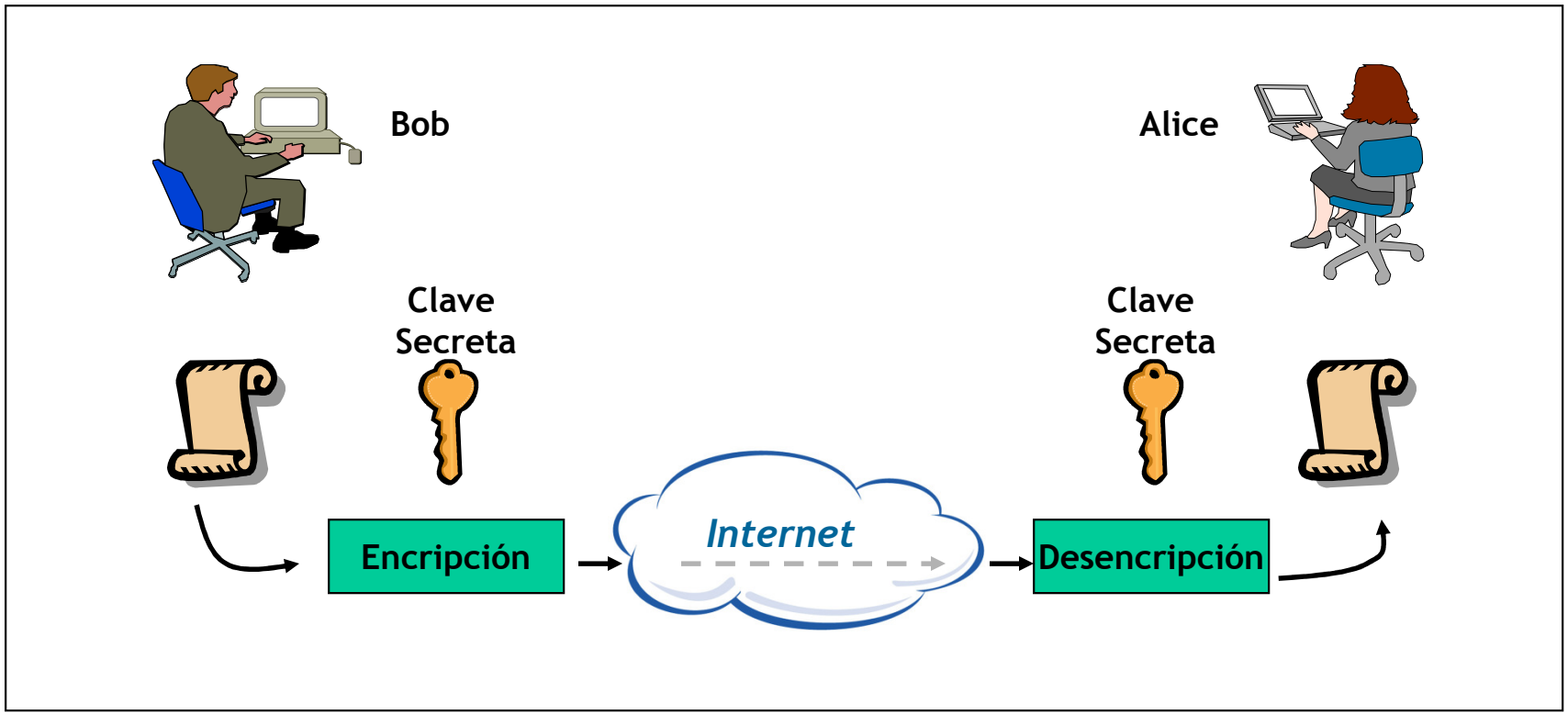
Criptografía

Longitud de la clave	Cantidad de Combinaciones
40	$2^{40} = 1.099.511.627.776$
56	$2^{56} = 7.2057 * 10^{16}$
64	$2^{64} = 1.8446 * 10^{19}$
112	$2^{112} = 5.1922 * 10^{33}$
128	$2^{128} = 3.4028 * 10^{38}$

Encripción Simétrica

Conocida como encripción de “clave secreta” utiliza una clave común y el mismo algoritmo criptográfico para encriptar y desencriptar el mensaje

Encripción Simétrica



Encripción Simétrica

Algunos de los algoritmos más conocidos de encripción simétrica son:

- Data Encryption Standard (DES)
- 3DES (triple DES)
- Rivest Cipher 4 (RC-4)
- International Data Encryption Algorithm (IDEA)
- AES (Advanced Encryption Standard) 128/192/256

DES es el esquema de encripción más ampliamente utilizado. Opera con mensajes de 64 bytes de longitud. 3DES es una alternativa a DES que hace más difícil un ataque por fuerza bruta. Toma un bloque de 64 bytes y encripta/desencripta/encripta con 1, 2 o 3 claves diferentes.

DES y 3DES son de dominio público y están públicamente disponibles

Encripción Asimétrica

Conocida como encripción de “Encripción de Clave Pública”

Los extremos pueden utilizar el mismo algoritmo o uno diferente pero complementario para encriptar y desencriptar la información

Dos valores de clave diferentes, pero complementarios una clave pública y una clave privada

Encripción Asimétrica

Algunos de los usos más comunes de los algoritmos de clave pública son :

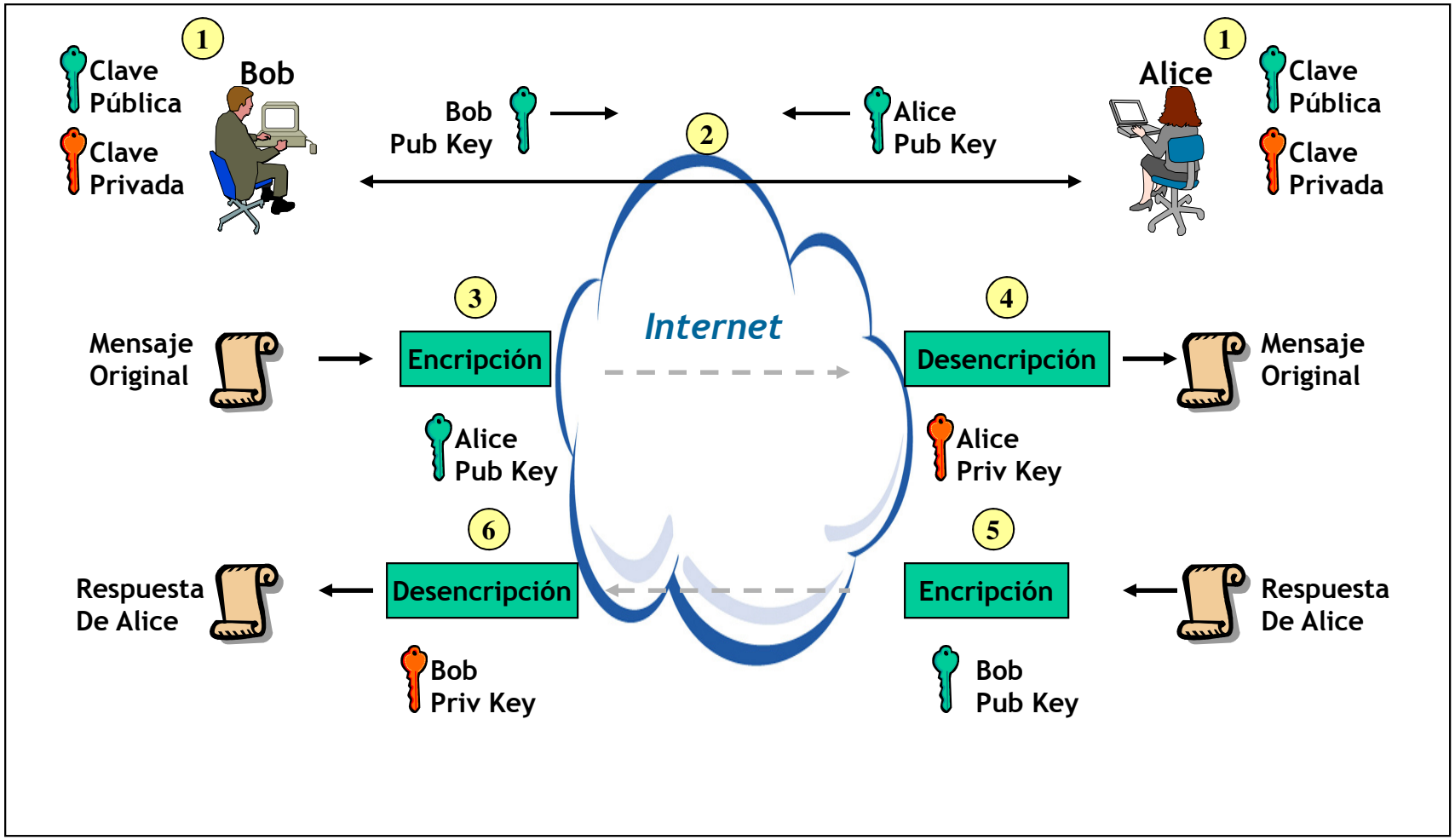
- Integridad de los datos
- Confidencialidad de los datos
- No repudio del emisor
- Autenticación del emisor

Encripción Asimétrica

Pasos a seguir para garantizar la confidencialidad:

1. Bob y Alice crean su par de claves pública/privada
2. Bob y Alice intercambian sus claves públicas
3. Alice escribe un mensaje a Bob y utiliza la ***Clave Pública*** de Bob para encriptar el mensaje. Luego envía los datos encriptados a Bob a través de Internet
4. Bob utiliza su ***Clave Privada*** para desencriptar la información

Encripción Asimétrica



Encripción Asimétrica

El mecanismo anterior garantiza la integridad y la confidencialidad

Confidencialidad

Está garantizada, ya que solo Bob conoce su clave privada y es capaz de desencriptar el mensaje

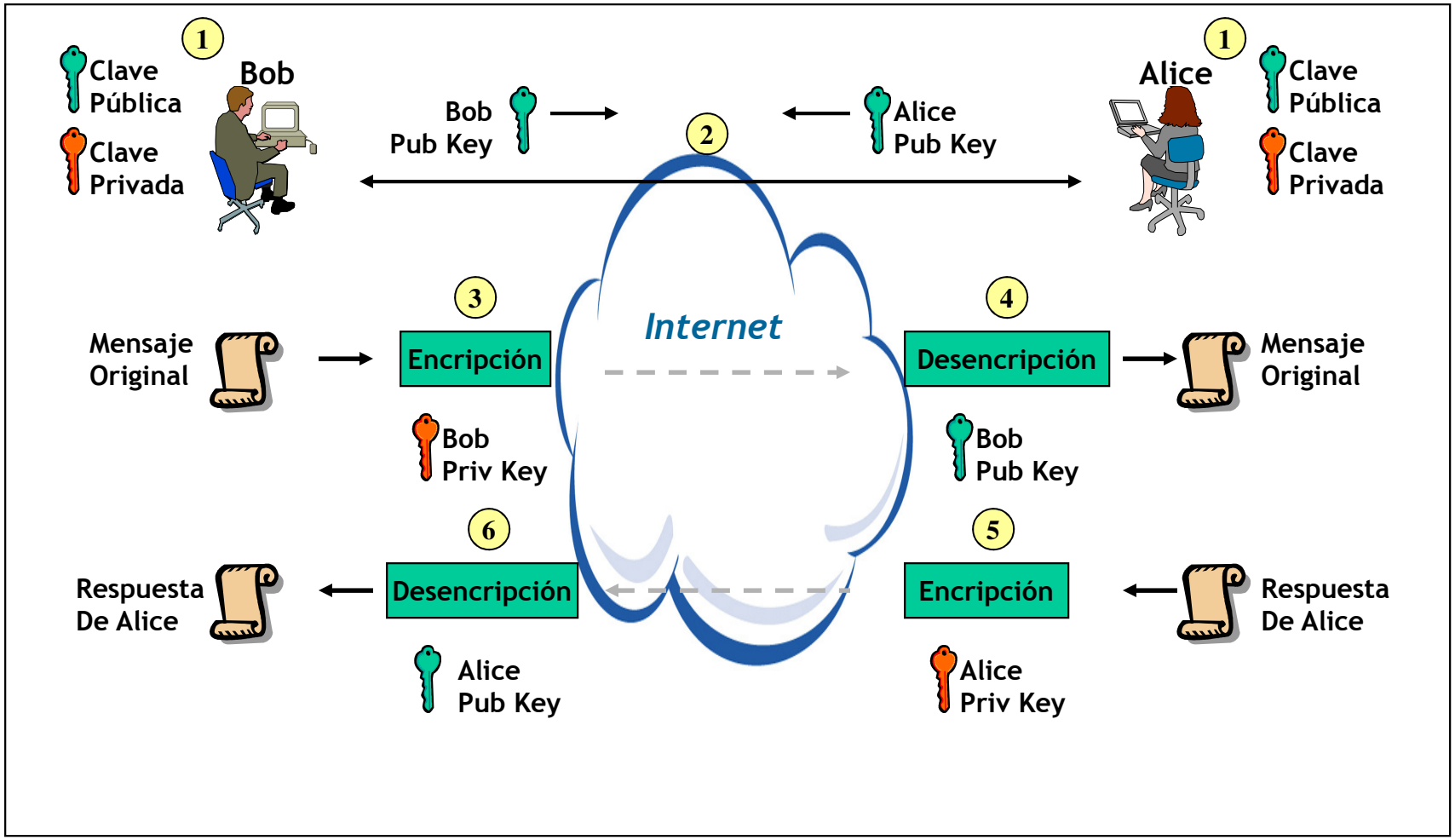
Integridad

Para alterar el mensaje, se necesitaría nuevamente la clave privada de Bob

El mecanismo no garantiza la autenticación ni el no-repudio ya que cualquier atacante podría enviar un mensaje pretendiendo ser Alice.

Tan solo necesita la clave pública de Bob, la cual es conocida

Encripción Asimétrica



Encripción Asimétrica

Autenticación

Está garantizada, ya que solo Bob y Alice conocen sus propias claves privadas

No-Repudio

Ni Bob, ni Alice pueden negar que el mensaje fue enviado por ellos, siempre que sus claves no hayan sido divulgadas

Si queremos garantizar un intercambio autenticado, junto con confidencialidad e integridad, debe realizarse una doble encripción.

Alice encriptaría su mensaje con la clave pública de Bob y luego encriptarla nuevamente con su clave privada. De esta manera cualquiera podría desencriptar el primer mensaje, pero solo Bob será capaz de desencriptar el segundo mensaje con su clave privada

Funciones de Hash

Una función de Hash toma una entrada de longitud arbitraria y genera una salida de longitud fija

La salida, de longitud fija, se llama “Digest”

Un algoritmo para ser considerado como una función de Hash, debe cumplir determinados requisitos:

- ***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 que generen el mismo Digest
- ***One way***: Para un Digest dado, debe ser muy difícil, sino imposible acertar el mensaje de entrada

Funciones de Hash

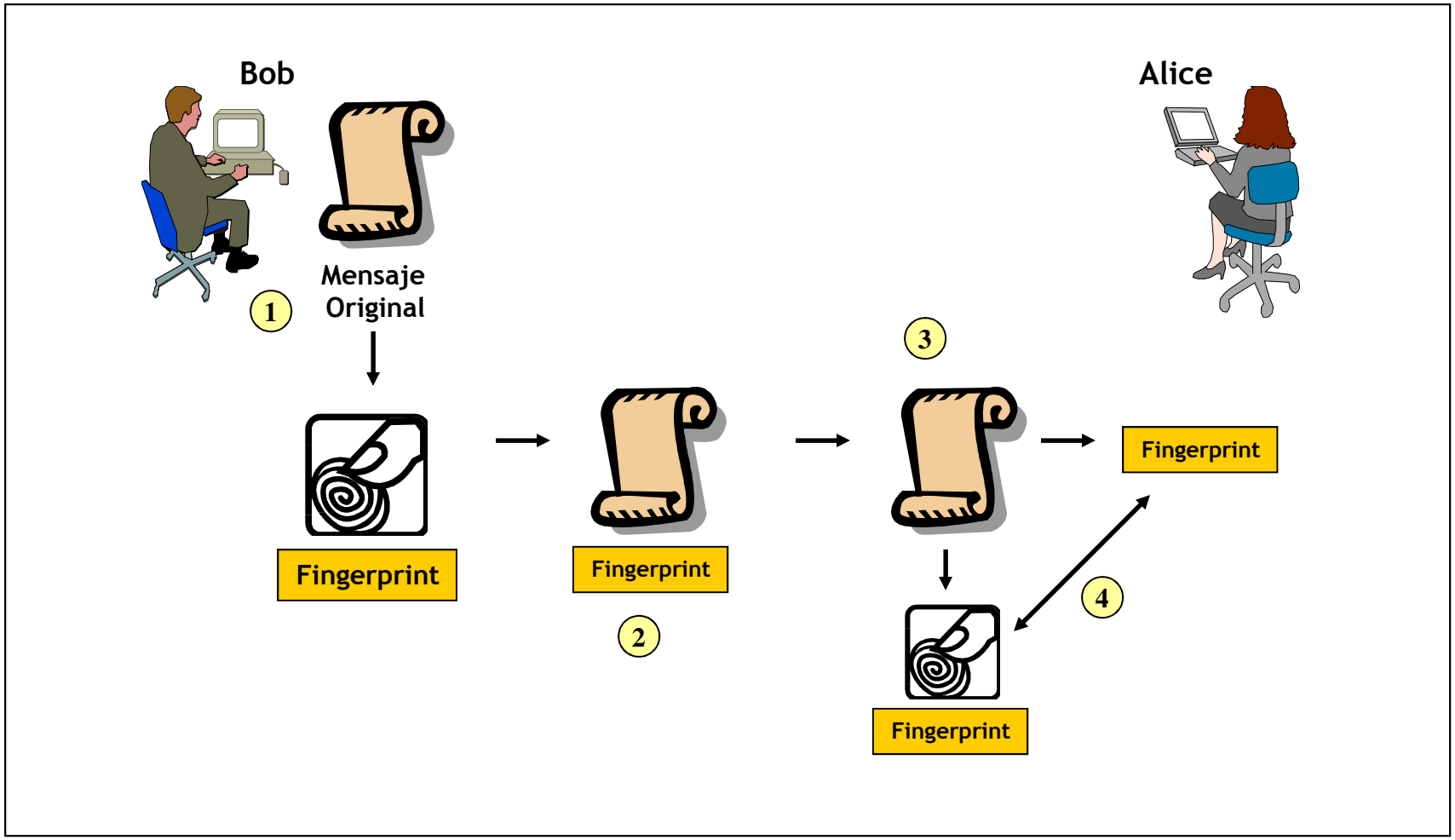
Las funciones de Hash garantiza la integridad del mensaje

Las funciones de Hash más comunes con:

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

MD5 procesa su entrada en bloques de 512 bits y genera un Digest de 128 bits. SHA tambien procesa la entrada de a 512 bits y produce un Digest de 160 bits (requiere de mayor poder de procesamiento y corre más lento)

Funciones de Hash

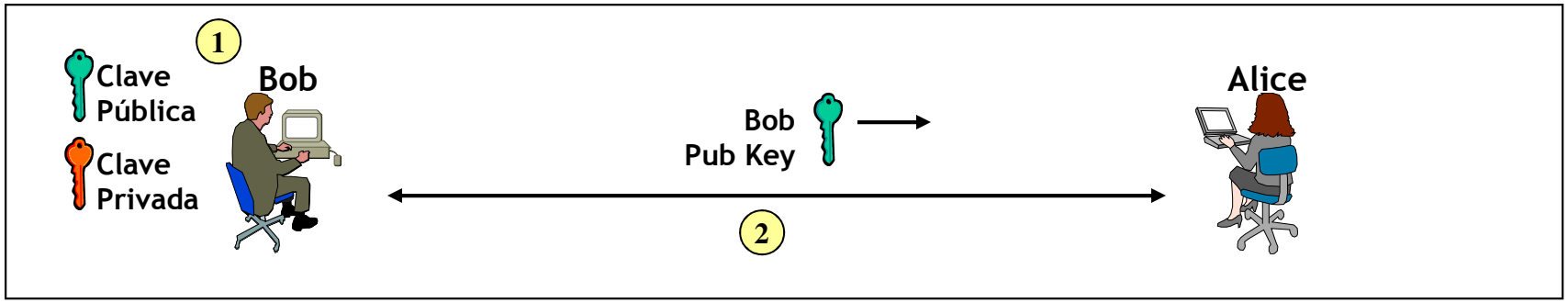


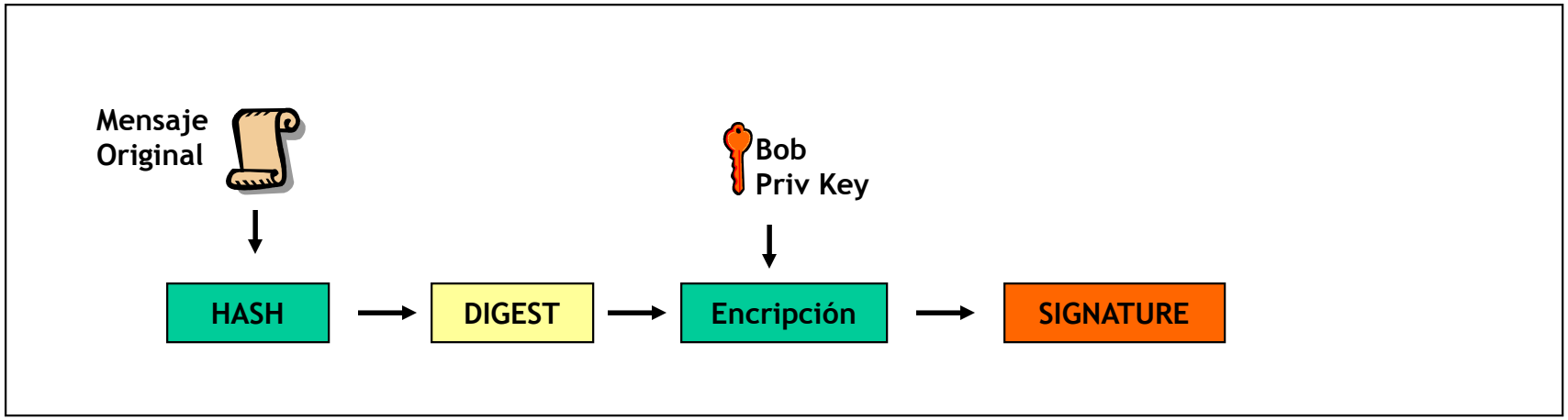
Firma Digital

Una Firma Digital es un Digest encriptado que se adiciona a un documento. Puede utilizarse para:

- Confirmar la identidad del emisor
- Garantizar la integridad del documento

Firma Digital





Firma Digital

Verificación de la Firma Digital