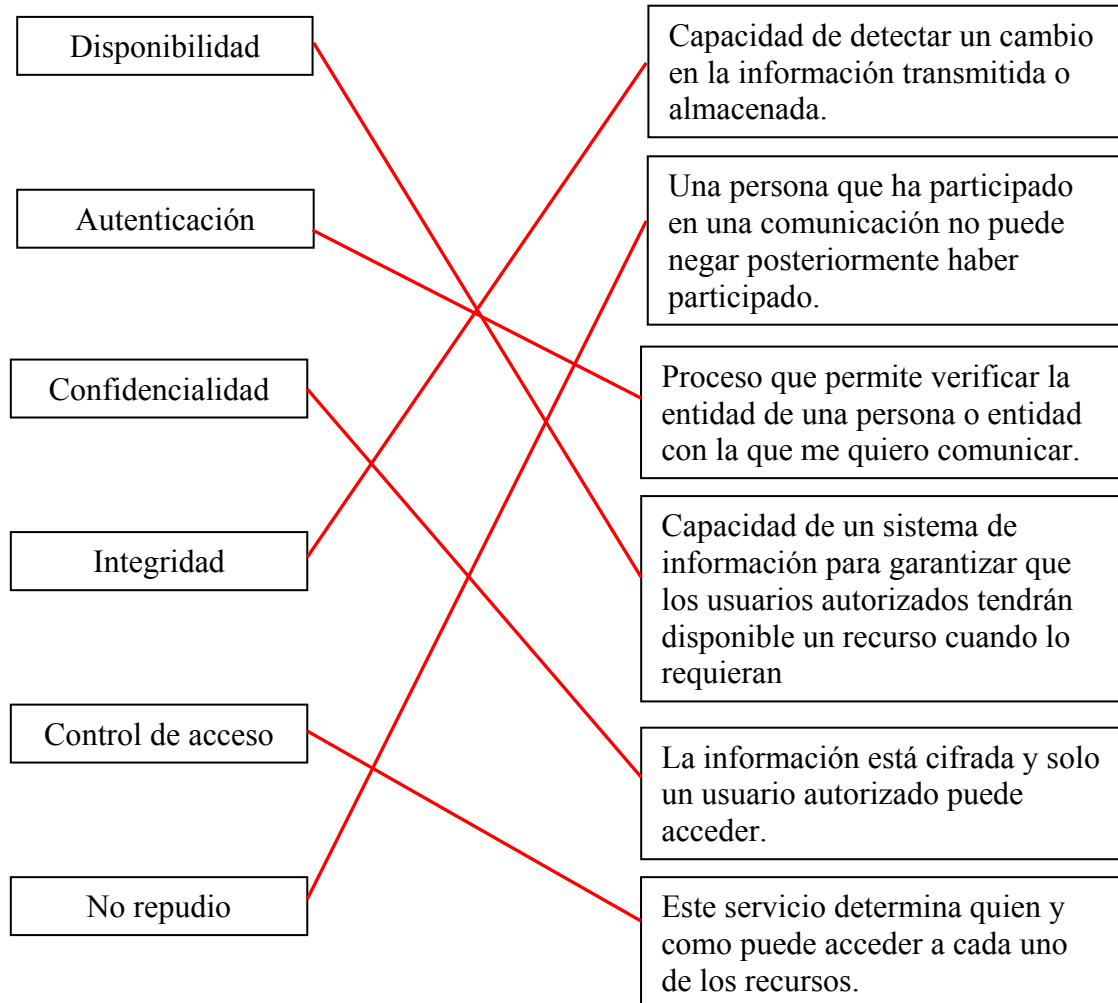


**1. Relaciona los conceptos de la columna izquierda con las definiciones correspondientes en la derecha.**



## 2. Cifrar y descifrar un texto utilizando una tabla de conversión (denominado cifrado de sustitución).

Texto en claro	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Alfabeto del criptograma	Z	V	I	R	E	A	B	C	D	F	G	H	J	K	L	M	N	O	P	Q	S	T	U	W	X	Y

**Cifra el texto:** (quoting Jan Werich – famous Czech writer, actor etc.):

EN UN LUGAR DE LA MANCHA

**EK SK HSBZO RE HZ JZKICZ**

**Descifra el criptograma:**

RE ISXL KLJVOE KL NSDEOL ZILORZOJE

**DE CUYO NOMBRE NO QUIERO ACORDARME**

## 3. Modica las siguientes frases de forma que la sentencia sea correcta.

Una de las propiedades caracterísiticas del cifrado ( ~~simétrico~~ **asimétrico** ) es su clave ( ~~larga~~ **corta** ).

Una de las propiedades caracterísiticas del cifrado ( ~~simétrico~~ **asimétrico** ) es su clave ( ~~larga~~ **corta** ).

El cifrado ( ~~simétrico~~ **asimétrico** ) es entre **100 y 1000** veces más ( ~~rápido~~ **lento** ) que el cifrado ( ~~simétrico~~ **asimétrico** ).

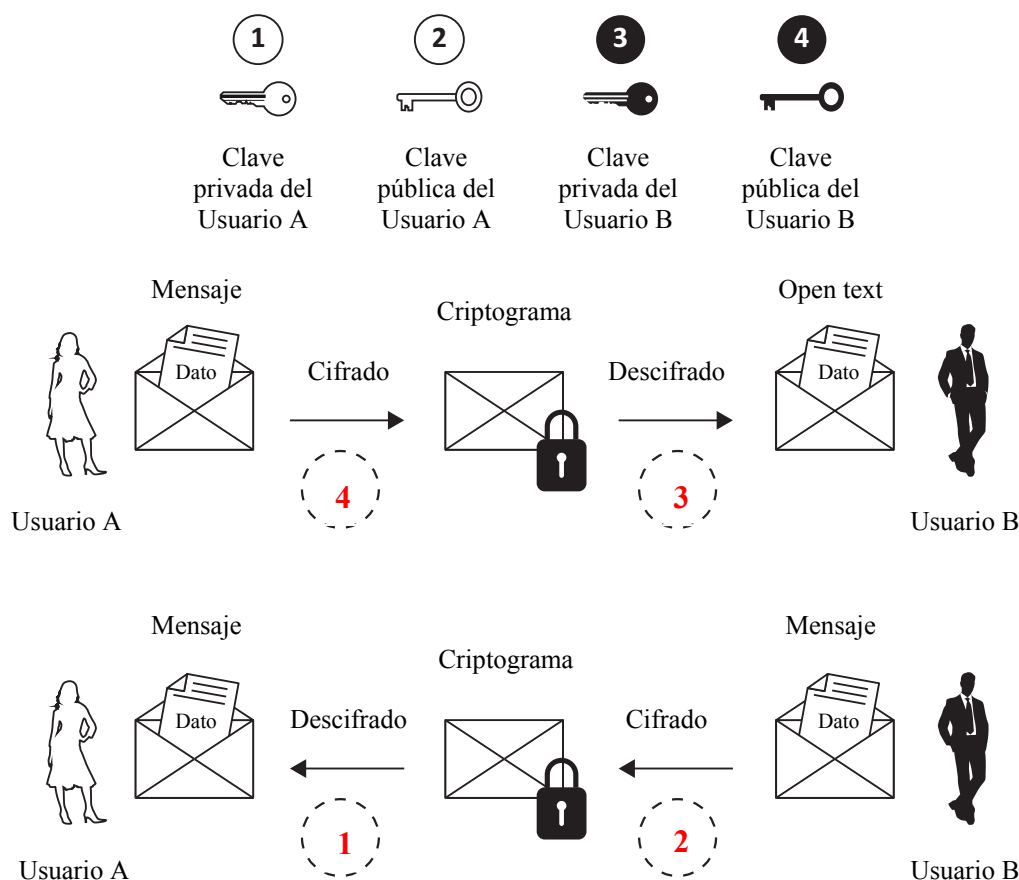
El cifrado ( ~~simétrico~~ **asimétrico** ) es entre **100 y 1000** veces más ( ~~rápido~~ **lento** ) que el cifrado ( ~~simétrico~~ **asimétrico** ).

El cifrado ( ~~simétrico~~ **asimétrico** ) ( ~~puede~~ **no puede** ) utilizarse en la generación de firmas digitales.

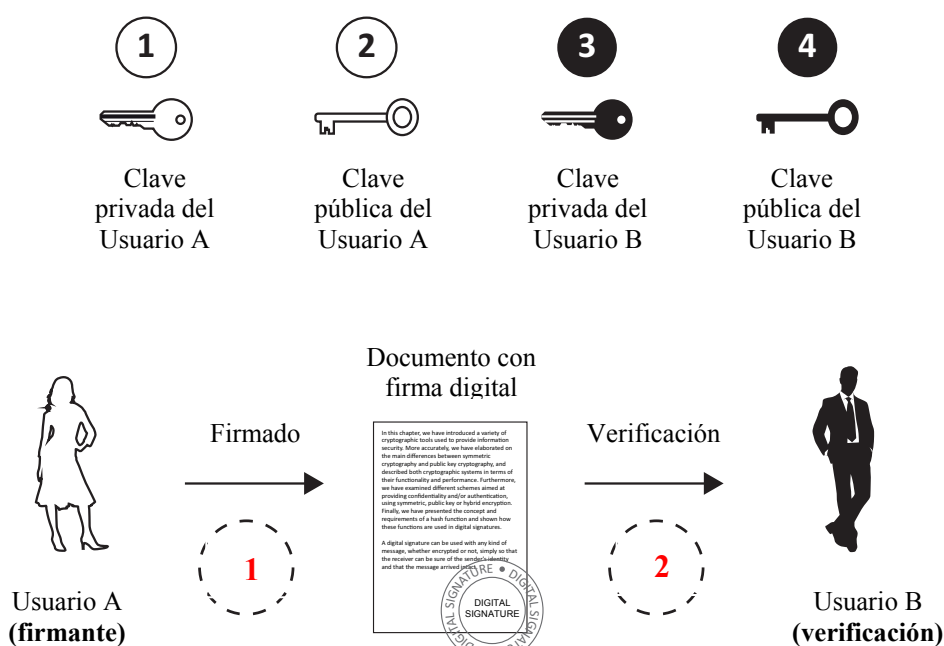
El cifrado ( ~~simétrico~~ **asimétrico** ) ( ~~puede~~ **no puede** ) utilizarse en la generación de firmas digitales



4. En la siguiente imagen señala las claves que deben ser utilizadas cuando las entidades que se comunican desean utilizar criptografía asimétrica para la transmisión confidencial de un documento.



5. En la siguiente imagen señala las claves que deben ser utilizadas cuando se debe generar y verificar una firma digital.



**6. Rellena las casillas con los numeros de frases correctas correspondientes a funciones de hash.**

**Las funciones de hash deben satisfacer los siguientes requisitos:**

3
6
8

- 1 – La longitud mínima de la entrada debe ser de 1024 bits **(no)**
- 2 – La longitud de salida es variable **(no)**
- 3 – La longitud de salida es constante **(sí)**
- 4 – Se puede utilizar la función hash inversa para recuperar los datos originales **(no)**
- 5 – Dos mensajes de entrada diferentes siempre producen resultados (los denominados hash) diferentes **(no, puede haber colisiones)**
- 6 – Las funciones de hash se utilizan habitualmente para generar firmas digitales **(sí)**
- 7 – Las funciones de hash se utilizan habitualmente para cifrar datos **(no)**
- 8 – Su objetivo es generar una salida única a partir de un mensaje de entrada **(sí)**

---

**7. Modifica la siguiente frase de modo que la sentencia sea cierta**

El cifrado simétrico usa ( **la misma clave** ) para el cifrado y descifrado.  
~~dos claves distintas~~