EJERCICIO C2/1

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

Disponibilidad	Capacidad de detectar un cambio en la información transmitida o almacenada.
Autenticación	Una persona que ha participado en una comunicación no puede negar posteriormente haber participado.
Confidencialidad	Proceso que permite verificar la entidad de una persona o entidad con la que me quiero comunicar.
Integridad	Capacidad de un sistema de información para garantizar que los usuarios autorizados tendrán disponible un recurso cuando lo requieran
Control de acceso	La información está cifrada y solo un usuario autorizado puede acceder.
No repudio	Este servicio determina quien y como puede acceder a cada uno de los recursos.

Programa de acción en el ámbito del aprendizaje permanente

El presente proyecto ha sido financiado con el apoyo de la Comisión Europea. Esta publicación (comunicación) es responsabilidad exclusiva de su autor. La Comisión no es responsable del uso que pueda hacerse de la información aquí difundida.

EJERCICIO C2/1

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

Descifra el criptograma:

RE ISXL KLJVOE KL NSDEOL ZILORZOJE

---

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).

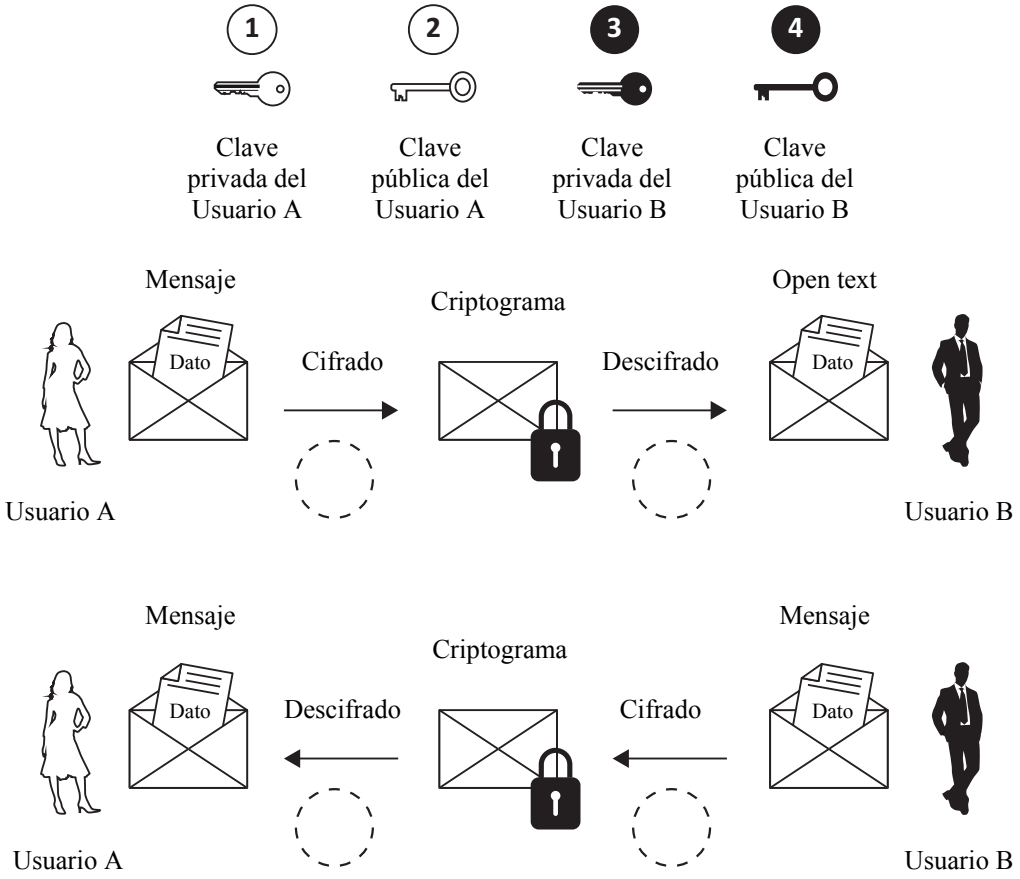
El cifrado (simétrico / asimétrico) es entre _____ veces más (rápido / lento) que el cifrado (simétrico / asimétrico).

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

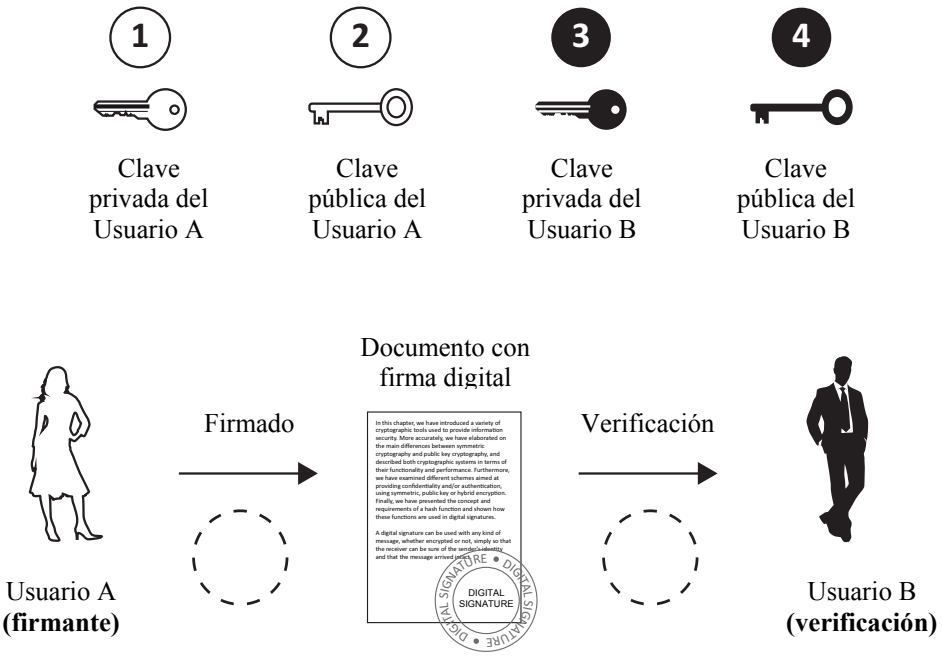
Programa de acción en el ámbito del aprendizaje permanente

El presente proyecto ha sido financiado con el apoyo de la Comisión Europea. Esta publicación (comunicación) es responsabilidad exclusiva de su autor. La Comisión no es responsable del uso que pueda hacerse de la información aquí difundida.

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 sed debe generar y verificar una firma digital.



Programa de acción en el ámbito del aprendizaje permanente

El presente proyecto ha sido financiado con el apoyo de la Comisión Europea. Esta publicación (comunicación) es responsabilidad exclusiva de su autor. La Comisión no es responsable del uso que pueda hacerse de la información aquí difundida.

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

Las funciones de hash deben satisfacer los siguientes requisitos:

1 – La longitud mínima de la entrada debe ser de 1024 bits
2 – La longitud de salida es variable
3 – La longitud de salida es constante
4 – Se puede utilizar la función hash inversa para recuperar los datos originales
5 – Dos mensajes de entrada diferentes siempre producen resultados (los denominadso hash) diferentes
6 – Las funciones de hash se utilizan habitualmente para generar firmas digitales
7 – Las funciones de hash se utilizan habitualmente para cifrar datos
8 – Su objetivo es generar una salida única a partir de un mensaje de entrada

---

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

El cifrado simétrico usa (la misma clave / dos claves distinas) para el cifrado y descifrado.

Programa de acción en el ámbito del aprendizaje permanente

El presente proyecto ha sido financiado con el apoyo de la Comisión Europea. Esta publicación (comunicación) es responsabilidad exclusiva de su autor. La Comisión no es responsable del uso que pueda hacerse de la información aquí difundida.