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

Capacidad de detectar un cambio en la información transmitida o almacenada.

Este servicio determina quien y como puede acceder a cada uno de los recursos.

Capacidad de un sistema de información para garantizar que los usuarios autorizados tendrán disponible un recurso cuando lo requieran

Control de acceso

Confidencialidad

Integridad

No repudio

Disponibilidad

Autenticación

Una persona que ha participado en una comunicación no puede negar posteriormente haber participado.

Proceso que permite verificar la entidad de una persona o entidad con la que me quiero comunicar.

La información está cifrada y solo un usuario autorizado puede acceder.

1. 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 |

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

Una de las propiedades caracterísiticas del cifrado es su clave.

Una de las propiedades caracterísiticas del cifrado es su clave .

El cifrado es entre **100 y 1000** veces más que el cifrado .

El cifrado es entre **100 y 1000** veces más que el cifrado .

El cifrado utilizarse en la generación de firmas digitales.

El cifrado utilizarse en la generación de firmas digitales

1. 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.

sifrovani1a.eps

Criptograma

Criptograma

**2**

**3**

**4**

**1**

Usuario A

Usuario B

Usuario B

Usuario A

Dato

Dato

Dato

Dato

Cifrado

Descifrado

Descifrado

Cifrado

Mensaje

Mensaje

Open text

Mensaje

Clave pública del Usuario B

Clave privada del Usuario B

Clave pública del Usuario A

Clave privada del Usuario A

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

sifrovani2a.eps

Usuario B

**(verificación)**

Clave privada del Usuario A

Clave privada del Usuario B

Clave pública del Usuario B

Clave pública del Usuario A

DIGITAL

SIGNATURE

Documento con firma digital

Verificación

Firmado

Usuario A

**(firmante)**

**1**

**2**

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

|  |
| --- |
| 3 |
| 6 |
| 8 |
|  |
|  |
|  |

Las funciones de hash deben satisfacer

los siguientes requisitos:

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 denominadso 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)

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

El cifrado simétrico usa para el cifrado y descifrado.