

1. Modifique los siguientes textos de manera que las afirmaciones sean ciertas.

El emisor y el receptor no tienen que compartir ninguna clave secreta cuando se usa criptografía $\left(\begin{array}{c} \text{simétrica} \\ \text{de clave pública} \end{array} \right)$.

Para verificar una firma digital, es necesaria $\left(\begin{array}{c} \text{la clave privada del firmante} \\ \text{la clave pública del firmante} \\ \text{la clave privada del receptor} \\ \text{la clave pública del receptor} \end{array} \right)$.

La longitud de clave en criptografía simétrica es $\left(\begin{array}{c} \text{más corta} \\ \text{más larga} \end{array} \right)$ que en algoritmos de clave pública.

En criptografía simétrica, el proceso de cifrado es $\left(\begin{array}{c} \text{más lento} \\ \text{más rápido} \end{array} \right)$ que en algoritmos de clave pública.

La criptografía $\left(\begin{array}{c} \text{simétrica} \\ \text{de clave pública} \end{array} \right)$ usa $\left(\begin{array}{c} \text{la misma clave} \\ \text{distintas claves} \end{array} \right)$ para el cifrado y el descifrado.

La criptografía $\left(\begin{array}{c} \text{simétrica} \\ \text{de clave pública} \end{array} \right)$ usa $\left(\begin{array}{c} \text{la misma clave} \\ \text{distintas claves} \end{array} \right)$ para el cifrado y el descifrado.

En cifrado híbrido, los datos de usuario son cifrados usando algoritmos $\left(\begin{array}{c} \text{simétrica} \\ \text{de clave pública} \end{array} \right)$.

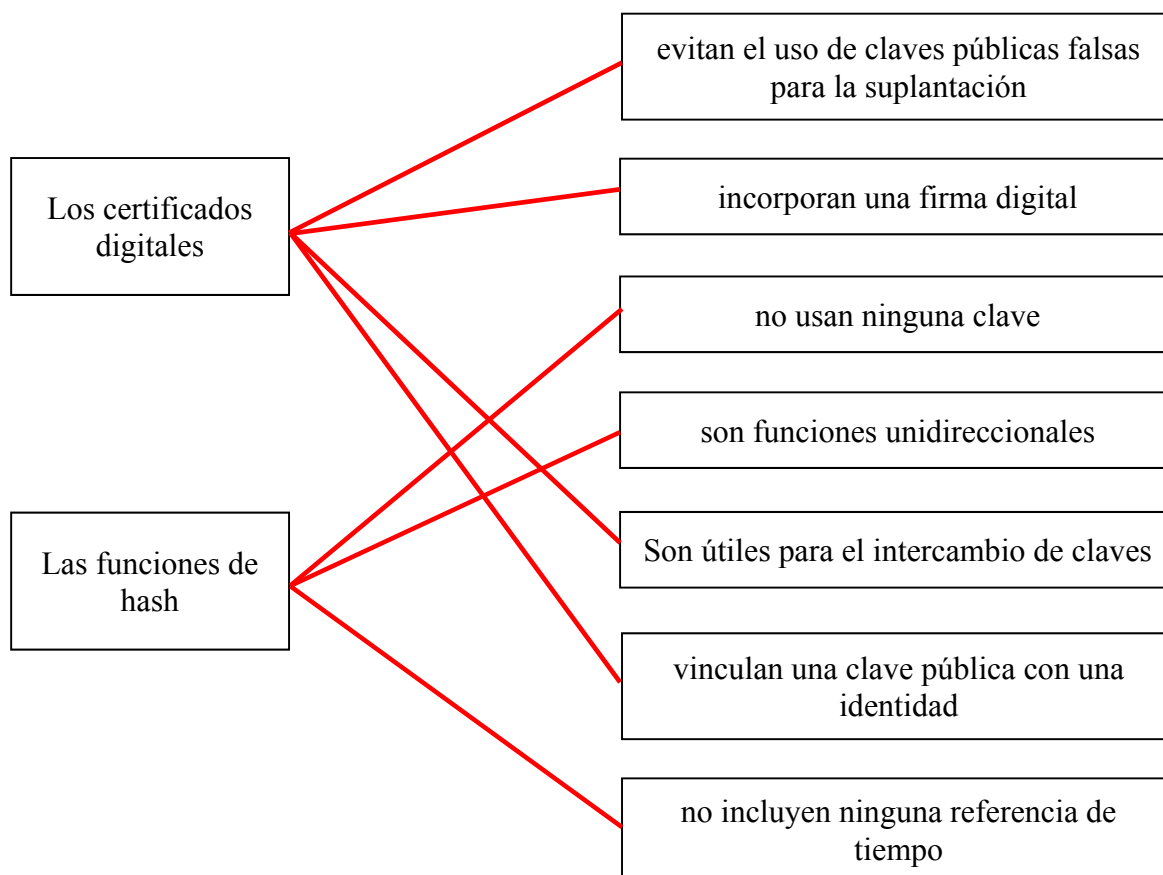
En cifrado híbrido, la $\left(\begin{array}{c} \text{la clave privada del emisor} \\ \text{la clave pública del emisor} \\ \text{la clave privada del receptor} \\ \text{la clave pública del receptor} \end{array} \right)$ se usa para el cifrado de $\left(\begin{array}{c} \text{datos de usuario} \\ \text{clave de sesión} \end{array} \right)$.

2. Marca las frases verdaderas.

- ☒ La firma digital debe ser un patrón de bits que depende del mensaje firmado.
- ☐ El proceso de firma digital debe ser relativamente fácil sin la clave privada del firmante.
- ☒ La falsificación de la firma digital debe ser computacionalmente imposible, ya sea mediante la construcción de un nuevo mensaje para una firma digital existente o mediante la construcción de una firma digital fraudulenta para un mensaje dado.
- ☐ Dada una firma digital, es posible encontrar el mensaje.
- ☒ La clave pública del firmante es necesaria para verificar su firma digital.



3. Asigne los términos de la columna de la izquierda a las propiedades correspondientes de la derecha (una o más)



4. Rellena la siguiente tabla indicando el número de las frases correctas relativas a mecanismos de ataques

1
3
4

- 1** – El análisis de tráfico se refiere al proceso de interceptar y examinar los mensajes con el fin de deducir información a partir de los patrones de la comunicación.
- 2** – Los ataques a servidor se refieren a todo tipo de ataques destinados a saturar a un ordenador o una red de tal manera que los usuarios legítimos de dicho ordenador o red no puedan utilizarlo.
- 3** – Los ataques basados en protocolo se aprovechan de las debilidades conocidas (o desconocidas) en los servicios de red.
- 4** – En los ataques de hombre en el medio (MitM), los intrusos interceptan las comunicaciones entre dos entidades, por lo general un usuario final y un sitio web.
- 5** – Los ataques de denegación de servicio se aprovechan de las vulnerabilidades de los sistemas operativos del ordenador de la víctima o en cómo el sistema está configurado y administrado.