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 (simétrica / de clave pública).

Para verificar una firma digital, es necesaria (la clave privada del firmante / la clave pública del firmante / la clave privada del receptor / la clave pública del receptor).

La longitud de clave en criptografía simétrica es (más corta / más larga) que en algoritmos de clave pública.

En criptografía simétrica, el proceso de cifrado es (más lento / más rápido) que en algoritmos de clave pública.

La criptografía (simétrica / de clave pública) usa (la misma clave / distintas claves) para el cifrado y el descifrado.

En cifrado híbrido, los datos de usuario son cifrados usando algoritmos (simétrica / de clave pública).

En cifrado híbrido, la (la clave privada del emisor / la clave pública del emisor / la clave privada del receptor / la clave pública del receptor) se usa para el cifrado de (datos de usuario / clave de sesión).

---

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.

Erasmus+
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.

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

Los certificados digitales	evitan el uso de claves públicas falsas para la suplantación
	incorporan una firma digital
	no usan ninguna clave
	son funciones unidireccionales
Las funciones de hash	Son útiles para el intercambio de claves
	vinculan una clave pública con una identidad
	no incluyen ninguna referencia de tiempo

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

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.

Erasmus+
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.