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

Uno de los mayores problemas de la criptografía (simétrica / de clave pública) es el proceso de transferir las claves al destinatario.

La criptografía (simétrica / de clave pública) (puede / no puede) ser usada para crear firmas digitales.

Cuando se aplica el modo de operación (ECB / CBC), la información estructural del texto en claro puede quedar comprometida.

Cuando se aplica el modo de operación CBC, los errores de propagación (si / no) están limitados.

En caso de errores en el texto cifrado, cuando se usa el modo de operación (CFB / OFB / CTR), estos errores (se propagan / no se propagan) en el texto en claro.

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.

2. Asigne los términos de la columna de la izquierda a las definiciones de la derecha

Criptografía de clave simétrica	Usa un flujo de claves generado independientemente del texto en claro y del texto cifrado
Cifrado en flujo	Pueden ser algoritmos simétricos o de clave pública
Cifrado en flujo	Pueden ofrecer por separado confidencialidad y autenticación
Cifrado en bloque	Siempre son algoritmos de clave simétrica.
Cifrado en flujo autosincronizante	Usa un flujo de claves que depende del texto cifrado
Cifrado en flujo síncrono	Opera con transformaciones variantes en el tiempo sobre símbolos individuales del texto en claro
Criptografía de clave pública	Siempre ofrece simultáneamente confidencialidad y autenticación

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. Marca las frases verdaderas.

☐ La firma digital sólo depende del autor, no depende del mensaje.

☐ La firma digital debe utilizar información única del emisor, para evitar tanto la falsificación como el repudio.

☐ La salida de una función hash tiene una longitud fija.

☐ Dado un mensaje, es fácil de encontrar su hash y viceversa.

☐ Es computacionalmente imposible encontrar dos mensajes distintos cuyo hash sea idéntico.

☐ Mensajes diferentes siempre tienen diferentes valores hash.

---

4. Clasifica los siguientes ataques como activos o pasivos.

Captura, suplantación, análisis de tráfico, repetición, denegación de servicio, modificación

Activo	
Pasivo	

---

5. Rellena la siguiente tabla indicando el número de las frases correctas relativas a certificados digitales.

1 – Un certificado digital contiene la clave secreta de un sujeto o titular del certificado, así como los datos de identificación de dicho sujeto titular.

2 – Los certificados digitales se firman con la clave privada de una autoridad de certificación (CA).

3 – Sólo la clave certificada por el certificado trabajará con la clave pública correspondiente que posee la entidad identificada por el certificado.

4 – Los certificados digitales vinculan una clave pública con una identidad.

5 – Un certificado digital contiene la clave pública de la autoridad de certificación (CA) correspondiente.

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.