

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

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

La criptografía (~~de clave pública~~ ^{simétrica}) (~~puede~~ ^{no puede}) ser usada para crear firmas digitales.

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

Cuando se aplica el modo de operación CBC, los errores de propagación (~~no~~ ^{si}) están limitados.

En caso de errores en el texto cifrado, cuando se usa el modo de operación (~~OFB~~ ^{CFB}), estos errores (~~no se propagan~~ ^{se propagan}) en el texto en claro.

En caso de errores en el texto cifrado, cuando se usa el modo de operación (~~CTR~~ ^{CFB}), estos errores (~~se propagan~~ ^{no se propagan}) en el texto en claro.

En caso de errores en el texto cifrado, cuando se usa el modo de operación (~~CTR~~ ^{CFB}), estos errores (~~no se propagan~~ ^{se propagan}) en el texto en claro.



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

3. Marca las frases verdaderas.

- ☐ La firma digital sólo depende del autor, no depende del mensaje.
- X** La firma digital debe utilizar información única del emisor, para evitar tanto la falsificación como el repudio.
- X** La salida de una función hash tiene una longitud fija.
- ☐ Dado un mensaje, es fácil de encontrar su hash y viceversa.
- X** 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	Suplantación, repetición, denegación de servicio, modificación
Pasivo	Captura, análisis de tráfico

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

2
4

- 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.

