

Nombre y apellidos:**Grupo:****Fecha:**

Instrucciones generales para las preguntas cerradas:

- Marca solamente la respuesta más apropiada en cada caso, en la tabla de respuestas
- No se tendrán en cuenta anotaciones fuera de la tabla de respuestas
- Todas las preguntas tienen el mismo valor.
- Hay una, y sólo una, respuesta correcta en cada pregunta.
- Responde solamente las preguntas en las que estés seguro. Una respuesta incorrecta resta un tercio del valor de una respuesta acertada. Una pregunta sin responder no resta puntos.

Instrucciones generales para las preguntas abiertas:

- Es necesario responder a la pregunta y justificar dicha respuesta
- Todas las preguntas tienen el mismo valor.

Puntuación:

- La parte tipo test es un 60 % de la nota
- La parte de preguntas abiertas es un 40% de la nota

1		2		3		4		5	
6		7		8		9		10	
11		12		13		14		15	
16		17							

-
1. Al cifrar un texto en claro con una de las claves de un sistema asimétrico, el texto cifrado resultante
- a) Se puede descifrar con la misma clave del sistema asimétrico
 - b) Tiene siempre la misma longitud (por ejemplo, 32 bytes para MD5)
 - c) Es igual al texto cifrado que se conseguiría con la otra clave asimétrica
 - d) Se puede descifrar con la otra clave del sistema asimétrica
-
2. Para mejorar el objetivo de "no repudio" de los envíos de información
- a) Basta con firmar los ficheros
 - b) Hay que firmar y encriptar los ficheros
 - c) Hay que enviar el fichero encriptado y sin encriptar, para su comparación
 - d) Basta con encriptar los ficheros
-
3. La criptografía híbrida
- a) Mezcla métodos de sustitución y transposición
 - b) Mezcla encriptación y firma
 - c) Mezcla métodos simétricos y asimétricos
 - d) Mezcla claves públicas y privadas
-
4. En un sistema de clave simétrica
- a) No es posible realizar firma electrónica
 - b) Es un problema el intercambio de claves, ya que si un tercero intercepta la clave puede cambiar las firmas electrónicas
 - c) No es un problema el intercambio de claves, ya que si un tercero intercepta la clave no puede descifrar los envíos
 - d) No es posible descifrar sin la clave privada
-
5. En un sistema de clave asimétrica
- a) Se encripta con una de las claves (privada o pública), y se descifra con la misma clave
 - b) Se encripta solamente con la clave pública, y se descifra solamente con la clave privada
 - c) Se encripta solamente con la clave privada, y se descifra solamente con la clave pública
 - d) Se encripta con una de las claves (privada o pública), y se descifra con la otra clave
-
6. Para conseguir una firma electrónica se necesita
- a) Una función resumen y un sistema de claves de tipo asimétrico
 - b) Un canal seguro y un sistema de claves asimétrico
 - c) Un canal seguro y un sistema de claves simétrico
 - d) Una función resumen y un sistema de claves de tipo simétrico
-
7. Son funciones resumen
- a) PKI, MD5
 - b) MD5, GPL
 - c) MD5, SHA1
 - d) SHA1, PKI
-
8. La desventaja de un sistema de clave asimétrica respecto de uno con clave simétrica es que
- a) Es menos seguro el intercambio de claves
 - b) Es menos seguro, porque es una tecnología más antigua
 - c) Es menos seguro, porque las claves son más cortas
 - d) Es más lento, por el tiempo de proceso
-
9. La desventaja de un sistema de clave simétrica respecto de uno con clave asimétrica es que
- a) Es más lento, por el tiempo de proceso
 - b) Es menos seguro, porque las claves son más cortas
 - c) Es menos seguro el intercambio de claves
 - d) Es más difícil y caro realizar programas que lo implementen

10. En una comunicación se comienza utilizando una clave asimétrica para intercambiar una clave simétrica. Esto se hace para

- a) Ahorrar tiempo de proceso, ya que las claves simétricas son más difíciles de computar
- b) Aumentar la confidencialidad
- c) Aumentar el objetivo de "no repudio"
- d) Ahorrar tiempo de proceso, ya que las claves asimétricas son más difíciles de computar

11. En un sistema de criptografía híbrida, como el estudiado en clase, hay

- a) 2 claves (dos públicas)
- b) 2 claves (una pública y una privada)
- c) 3 claves (una pública, una privada y una simétrica)
- d) 3 claves (dos públicas y una privada)

12. En un sistema de criptografía híbrida, como el estudiado en clase

- a) Una de las partes inventa sobre la marcha un par de claves (pública y privada)
- b) Una de las partes inventa sobre la marcha una clave privada
- c) Una de las partes inventa sobre la marcha una clave simétrica
- d) Una de las partes inventa sobre la marcha una clave pública

13. El "Cifrado del César" es

- a) Criptografía simétrica, porque se usa la misma clave para cifrar y descifrar
- b) Criptografía asimétrica, porque se usa distinto algoritmo para cifrar que para descifrar
- c) Criptografía estadística, porque se necesitan probar varias posibilidades

d) Criptografía híbrida, porque mezcla métodos manuales y automáticos

14. La autenticación consiste en

- a) firmar un documento
- b) verificar la identidad de un usuario
- c) usar métodos biométricos
- d) otorgar permisos a cierto usuario

15. Se dice de un certificado que es raíz si

- a) Es un certificado firmado por otro que tenga mayor nivel
- b) Es un certificado considerado seguro, que puede firmar otros certificados
- c) Es el certificado que se utilizó para instalar el sistema operativo
- d) Es el certificado asociado a la raíz del DNS (.)

16. En Linux, se puede encriptar

- a) Particiones y discos completos, incluso las particiones de inicio
- b) Particiones y discos completos, pero no las de inicio (para eso se crean "/" y "/home" en particiones separadas)
- c) Particiones completas
- d) Discos completos

17. En Windows, se puede encriptar

- a) Particiones y discos completos, incluso las particiones de inicio
- b) Particiones completas
- c) Particiones y discos completos, pero no las de inicio (para eso se crean "X:\windows" e "Y:\users" en particiones separadas)
- d) Discos completos

-
18. Describe cómo se realiza la comunicación utilizando criptografía híbrida (como en los protocolos SSL/TLS). Incluye un diagrama temporal como los utilizados en clase

a)