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) Tiene siempre la misma longitud (por ejemplo, 32 bytes para MD5)
   b) Se puede descifrar con la misma clave del sistema asimétrico
   c) Se puede descifrar con la otra clave del sistema asimétrica
   d) Es igual al texto cifrado que se conseguiría con la otra clave asimétrica

2. Para mejorar el objetivo de "no repudio" de los envíos de información

   a) Hay que firmar y encriptar los ficheros
   b) Hay que enviar el fichero encriptado y sin encriptar, para su comparación
   c) Basta con firmar los ficheros
   d) Basta con encriptar los ficheros

3. La criptografía híbrida

   a) Mezcla encriptación y firma
   b) Mezcla métodos simétricos y asimétricos
   c) Mezcla métodos de sustitución y transposición
   d) Mezcla claves públicas y privadas

4. En un sistema de clave simétrica

   a) No es posible desencriptar sin la clave privada
   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 desencriptar los envíos
   d) No es posible realizar firma electrónica

5. En un sistema de clave asimétrica

   a) Se encripta solamente con la clave privada, y se desencripta solamente con la clave pública
   b) Se encripta con una de las claves (privada o pública), y se desencripta con la otra clave
   c) Se encripta solamente con la clave pública, y se desencripta solamente con la clave privada
   d) Se encripta con una de las claves (privada o pública), y se desencripta con la misma clave

6. Para conseguir una firma electrónica se necesita

   a) Un canal seguro y un sistema de claves simétrico
   b) Una función resumen y un sistema de claves de tipo simétrico
   c) Una función resumen y un sistema de claves de tipo asimétrico
   d) Un canal seguro y un sistema de claves asimétrico

7. Son funciones resumen

   a) MD5, SHA1
   b) MD5, GPL
   c) SHA1, PKI
   d) PKI, MD5

8. La desventaja de un sistema de clave asimétrica respecto de uno con clave simétrica es que

   a) Es menos seguro, porque es una tecnología más antigua
   b) Es menos seguro el intercambio de claves
   c) Es más lento, por el tiempo de proceso
   d) Es menos seguro, porque las claves son más cortas

9. La desventaja de un sistema de clave simétrica respecto de uno con clave asimétrica es que

   a) Es más difícil y caro realizar programas que lo implementen
   b) Es más lento, por el tiempo de proceso
   c) Es menos seguro, porque las claves son más cortas
   d) Es menos seguro el intercambio de claves

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

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

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

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

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

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

13. El "Cifrado del César" es

    a) Criptografía estadística, porque se necesitan probar varias posibilidades
    b) Criptografía asimétrica, porque se usa distinto algoritmo para cifrar que para descifrar
    c) Criptografía simétrica, porque se usa la misma clave para cifrar y descifrar
    d) Criptografía híbrida, porque mezcla métodos manuales y automáticos

14. La autenticación consiste en

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

15. Se dice de un certificado que es raíz si

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

16. En Linux, se puede encriptar

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

17. En Windows, se puede encriptar

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