SEGURIDAD EN REDES DE COMUNICACIONES
5º curso Ing. Telecomunicación

APELLIDOS_____	No rellenar este espacio
NOMBRE_____	
DNI_____	

No rellenar este espacio
Correctas Incorrectas S/C

LEEME:

- El examen de teoría consta de 30 cuestiones tipo test.
- En el test, rodee la respuesta correcta con un círculo.
- Cada respuesta incorrecta del test resta ⅓ de una correcta.
- El examen de prácticas consta de 4 cuestiones.
- La duración total del examen es de 2 horas.
- No se admitirá ninguna respuesta a lápiz en el examen.

TEORIA [10 puntos]

1. Una técnica de transposición consiste en...
a) procesar el texto plano por bloques.
b) sustituir los elementos del texto plano por otros elementos.
c) reordenar los elementos del texto plano.
d) Ninguna respuesta es correcta.

2. Indique cuál de los siguientes no es un algoritmo de cifrado simétrico:
a) AES
b) DES
c) RC4
d) Ninguna respuesta es correcta.

3. En un algoritmo de cifrado asimétrico existe/n...
a) una única clave.
b) dos claves.
c) tantas claves como queramos.
d) Ninguna respuesta es correcta.

4. En el modo ECB (*Electronic CodeBook*) del algoritmo DES, donde cada bloque de 64 bits se cifra independientemente usando la misma clave...
a) Tendremos una vulnerabilidad si el mismo bloque de texto plano aparece más de una vez.
b) Tendremos una vulnerabilidad si usamos la misma clave para cifrar todos los bloques.
c) Tendremos una vulnerabilidad si no añadimos relleno en el último bloque de texto plano.
d) Ninguna respuesta es correcta.

5. Indique cuál de los siguientes representa el esquema de cifrado 3DES:
a) $Y=E_{K2}[E_{K1}(X)]$
b) $Y=E_{K3}[E_{K2}[E_{K1}(X)]]$
c) $Y= E_{K4}[E_{K3}[E_{K2}[E_{K1}(X)]]]$
d) Ninguna respuesta es correcta.
6. AES permite emplear claves de tamaño:

a) 64 bits
b) 128 bits
c) 512 bits
d) Todas las respuestas son correctas.

7. indique cuál de las siguientes respuestas es correcta:
   I. En implementaciones software, AES es en media tres veces más rápido que 3DES.
   II. En implementaciones hardware, AES es considerado un algoritmo más débil que 3DES.

a) I cierta, I cierta.
b) I cierta, II falsa.
c) I falsa, II cierta.
d) I falsa, II falsa.

8. Indique cuál de las siguientes respuestas es correcta:
   I. La criptografía de clave pública está basada en transposiciones y sustituciones.
   II. La criptografía de clave privada está basada en funciones matemáticas.

a) I cierta, I cierta.
b) I cierta, II falsa.
c) I falsa, II cierta.
d) I falsa, II falsa.

9. Sabiendo que el algoritmo RSA queda representado de la siguiente forma, indique cuál de las siguientes afirmaciones NO es correcta:

$$Y = X^e \bmod n$$
$$X = Y^d \bmod n$$

a) Si un atacante quiere obtener la clave privada a partir de la clave pública la única opción es hacer un ataque por fuerza bruta.
b) Los valores e y d deben ser primos relativos a $\Phi(n)$, donde $\Phi(n)$ es la función Totient de Euler.
c) Tanto emisor como receptor deben conocer el valor de n.
d) Todas las respuestas son correctas.

10. Dos entidades, A y B, desean obtener una clave secreta sin necesidad de enviarla por un medio que pueda poner en peligro la seguridad. Deciden emplear el método de Diffie-Hellman. La entidad A selecciona un número aleatorio x_A=2 y la entidad B selecciona x_B=3. El número primo escogido es 97 y la raíz primitiva es 5. ¿Cuál es el valor de la clave secreta?

a) 25
b) 28
c) 97
d) Ninguna respuesta es correcta.

11. Indique cuál de las siguientes respuestas es correcta:
a) El grupo elíptico $E_{23}(1,1)$ sólo puede incluir puntos dentro del cuadrante (1,1) a (23,23).
b) Para un mismo nivel de seguridad, el tamaño de una clave RSA es menor que el tamaño de una clave en ECC.
c) El punto generador G(x_1, y_1) será cualquiera en el que se cumplan que los valores de x_1 e y_1 deben ser primos.
d) Ninguna respuesta es correcta.

12. Indique cuál de las siguientes respuestas es correcta:

a) EL algoritmo RC4 es un algoritmo de cifrado caracterizado por su fácil implementación software.
b) El protocolo WEP garantiza su invulnerabilidad gracias al uso del algoritmo RC4.
c) RC4 no es un algoritmo de cifrado propietario.
d) Ninguna respuesta es correcta.

13. Indique cuál de la siguientes respuestas es correcta:
I. A3 es un algoritmo de autenticación empleado en GSM.
II. A5 es un algoritmo de cifrado empleado en GSM.
a) I cierta, II cierta.
b) I cierta, II falsa.
c) I falsa, II cierta.
d) I falsa, II falsa.

14. Un autentificador es...
a) un texto cifrado.
b) un MAC.
c) a) y b)
d) Ninguna respuesta es correcta.

15. ¿Cuál sería el orden correcto de los siguientes mensajes para un intercambio EAP? ($\rightarrow$ de usuario a autenticador; $\leftarrow$ de autenticador a usuario).
a) $\rightarrow$ REQUEST.IDENTITY
$\leftarrow$RESPONSE.IDENTITY
$\rightarrow$ REQUEST.MD5CHALLENGE
$\leftarrow$RESPONSE.NAK
$\rightarrow$ REQUEST.GENERICTOKENRING
$\leftarrow$RESPONSE.GENERICTOKENRING
$\rightarrow$ SUCCESS
b) $\rightarrow$ RESPONSE.IDENTITY
$\leftarrow$ REQUEST.GENERICTOKENRING
$\rightarrow$ RESPONSE.NAK
$\leftarrow$ REQUEST.MD5CHALLENGE
$\rightarrow$ RESPONSE.MD5CHALLENGE
$\rightarrow$ SUCCESS
c) $\leftarrow$ RESPONSE.IDENTITY
$\rightarrow$ RESPONSE.NAK
$\rightarrow$ REQUEST.MD5CHALLENGE
$\leftarrow$ RESPONSE.MD5CHALLENGE
$\rightarrow$ SUCCESS
d) Ninguna respuesta es correcta.

16. En Kerberos, un centro de distribución de claves consta de:
a) Servidores de reinos y servidor de emisión de nombres.
b) Servidores de principales y servidor de emisión de claves.
c) Servidor de autenticación y servidores de emisión de billetes.
d) Ninguna respuesta es correcta.

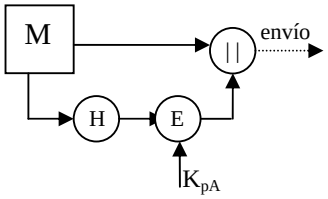
17. El *phising* es un ejemplo de...
a) Amenaza lógica.
b) Ingeniería social.
c) Catástrofe natural.
d) Ninguna respuesta es correcta.
18. Un certificado digital personal contiene...

a) la clave pública del usuario al que fue emitido el certificado.
b) la clave pública y la clave privada del usuario al que fue emitido el certificado.
c) la clave pública, la clave privada y la fecha de revocación de certificado del usuario al que fue emitido el certificado.
d) Ninguna respuesta es correcta.

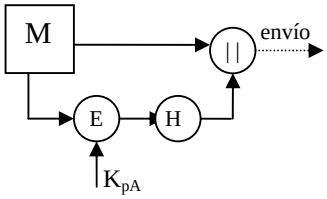
19. ¿Cuál de los siguientes algoritmos para calcular *hash* es más seguro frente a ataques por criptoanálisis? ¿Y por fuerza bruta?
a) MD5 y SHA1 respectivamente
b) SHA1 y MD5 respectivamente
c) RC4 y MD5 respectivamente
d) Ninguna respuesta es correcta.

20. Si los puertos de un switch (compatible con 802.1x) que realiza las funciones de autenticador están en estado NO AUTORIZADO significa que….
a) esos puertos permiten tráfico sólo si está destinado dentro de la red de área local.
b) esos puertos no permiten ningún tipo de tráfico, ya que así lo especifica el estándar 802.1x.
c) esos puertos permiten únicamente tráfico de inicialización (ej:DHCP) si lo permite el administrador de la red.
d) Ninguna respuesta es correcta.

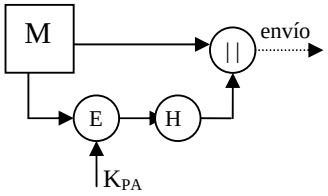
21. ¿Cuál de las siguientes figuras se corresponde con el proceso de firma digital?
Suponga que el mensaje lo envía el usuario A. M=Mensaje. H=hash. E=cifrado. ||=concaternar. K_{PA}=clave pública A. K_{pA}= clave privada A.



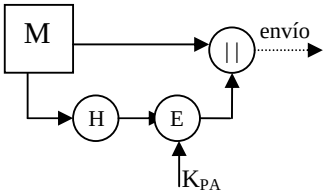
a)



b)



c)



d)

22. Cualquier circunstancia o evento que potencialmente puede causar un daño a una organización mediante la exposición, modificación o destrucción de información o mediante la denegación de servicios críticos es…
a) Una vulnerabilidad.
b) Una amenaza.
c) Un ataque.
d) Ninguna respuesta es correcta.

23. Indique cuál de las siguientes afirmaciones sobre el protocolo SET es falsa:

a) Es una especificación abierta de cifrado y seguridad.
b) Protege transacciones con tarjetas de crédito en Internet.
c) Es un sistema de pago.
d) El usuario (comprador) debe disponer de un certificado digital para poder usar SET.

24. La finalidad de la firma dual, utilizada en el protocolo SET, es permitir identificar la autenticidad ...
a) del comprador.
b) del vendedor.
c) de la pasarela de pagos.
d) Ninguna respuesta es correcta.

25. ¿Cuál de las siguientes acciones no es obligatoria en SSL?
a) Autenticación de servidor.
b) Autenticación de cliente.
c) Cifrado de sesiones.
d) Ninguna respuesta es correcta.

26. ¿Qué protocolo SSL es el encargado de proporcionar confidencialidad e integridad?
a) Change Cipher Spec.
b) Handshake.
c) Alert.
d) Ninguna respuesta es correcta.

27. Indique cuál de las siguientes es una diferencia entre el protocolo TLS y el protocolo SSL:
a) TLS emplea HMAC, SSL no.
b) TLS calcula todas las claves a partir de una clave denominada K_{previa}, SSL obtiene todas las claves mediante intercambios RSA o Diffie-Hellman.
c) TLS no emplea relleno en los bloques de datos a cifrar, SSL sí.
d) Ninguna respuesta es correcta.

28. El protocolo IPSec que proporciona confidencialidad se denomina:
a) ESP
b) AH
c) IKE
d) Ninguna respuesta es correcta.

29. Cuando utilizamos el protocolo IPSec entre pasarelas, o entre un host conectado a una pasarela de seguridad, estamos en modo:
a) Túnel.
b) Transporte.
c) Pasarela.
d) Ninguna respuesta es correcta.

30. Las asociaciones de seguridad IPSec se caracterizan por ser:
I. Unidireccionales.
II. Dependientes del protocolo.
a) I cierta, II cierta.
b) I cierta, II falsa.
c) I falsa, II cierta.
d) I falsa, II falsa.