GRADO EN INGENIERÍA TELEMÁTICA

SEGURIDAD EN REDES

FEBRERO 2014 (TIPO 1)

NOMBRE_____

DNI_____

No rellenar este espacio

IMPORTANTE:

- **El examen consta de 25 cuestiones tipo test y 2 problemas**
- **Cada respuesta incorrecta del test resta 1/3 de una correcta**
- **La duración del examen es de 2 horas**
- **No se admitirá ninguna respuesta a lápiz**

TEST (6 puntos)

1. Un certificado digital
   a) Contiene: clave pública del propietario, clave privada del propietario, identificador del algoritmo de firma del certificado y firma realizada por la autoridad certificadora (entre otros datos)
   b) Sirve para verificar la clave privada de su propietario
   c) Es obligatorio que los dos extremos de una comunicación SSL lo posean
   d) Ninguna respuesta es correcta

2. Si un atacante puede añadir registros en una base de datos (sin tener autorización para ello) estaremos hablando de una amenaza
   a) De interrupción
   b) De interceptación
   c) De modificación
   d) Ninguna respuesta es correcta

3. Si se emplea el protocolo EAP para autenticación, ¿cuántos mensajes son necesarios suponiendo una autenticación exitosa?
   a) 3
   b) 5
   c) 7
   d) Ninguna respuesta es correcta

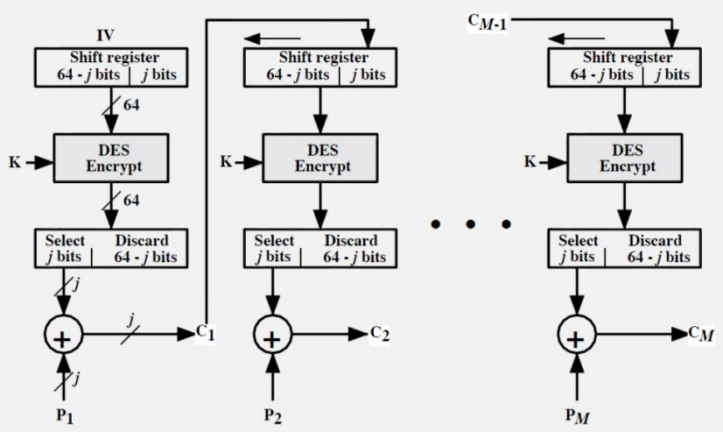
4. Indique cuál de las siguientes respuestas es correcta:
   I. En cualquier organización debe existir una política de seguridad que formalice el uso correcto e incorrecto de los recursos de la red de comunicación, las posibles amenazas contra el sistema y las medidas a adoptar para proteger al sistema de dichas amenazas.
   II. Los mecanismos de seguridad utilizados para implementar la política de seguridad elegida se dividen en mecanismos de prevención y de detección.
   a) I cierta, II cierta
   b) I cierta, II falsa
   c) I falsa, II cierta
   d) I falsa, II falsa

5. ¿De dónde se obtienen las subclaves necesarias para el proceso de cifrado/descifrado en DES?
   a) Del texto del primer bloque a cifrar
   b) Del vector inicialización (IV)
   c) De la clave compartida
   d) De una función pseudoaleatoria

6. Dos comunicantes Alice y Bob deciden usar el algoritmo Diffie-Hellman usando como número primo p = 11. Sabiendo que Alice escoge x_A=4 y conoce Y_B=8, ¿cuál es la clave compartida?
   a) Es necesaria más información para resolver esta cuestión.
   b) K=7
   c) K=11
   d) Ninguna respuesta es correcta

7. Indique cuál de las siguientes respuestas es correcta:
   I. TLS se puede emplear como protocolo de autenticación tanto en EAP como en IEEE 802.1x.
   II. En IEEE 802.1x, del suplicante al autenticador se usa el protocolo EAP sobre LAN o WLAN y del autenticador al servidor de autenticación se puede usar el protocolo RADIUS.
   a) I cierta, II cierta
   b) I cierta, II falsa
   c) I falsa, II cierta
   d) I falsa, II falsa

8. Si se produce un error de bit en la transmisión de un carácter cifrado con DES en modo CFB (j=8), ¿cuántos caracteres se descifrarán de forma incorrecta? (La figura muestra el cifrado del modo CFB, C ≡ texto cifrado, P ≡ texto plano)



   a) Ninguno
   b) Uno
   c) Dos
   d) Ninguna respuesta es correcta

9. Indique cuál de las siguientes opciones **no** es correcta:
   a) En el mismo hardware SHA-1 es más rápido que MD5
   b) Tanto SHA-1 como MD5 funcionan bien en arquitecturas de 32 bits
   c) SHA-1 es más fuerte frente a ataques por fuerza bruta comparado con MD5
   d) Ninguna respuesta es correcta

10. Sea E la curva elíptica $y^2 \equiv x^3+x+6 \pmod{11}$, indique cuál de los siguientes puntos pertenece al grupo elíptico $E_{11}(1,6)$:
   a) (5,9)
   b) (6,4)
   c) $E_{11}(1,6)$ no puede ser un grupo elíptico porque sus coeficientes a y b no cumplen el requisito necesario
   d) Ninguna respuesta es correcta

11. En los algoritmos de cifrado en flujo, ¿qué se usa como clave?
   a) La semilla del generador pseudoaleatorio capaz de generar secuencias criptográficamente aleatorias
   b) El primer número generado mediante el generador pseudoaleatorio capaz de generar secuencias criptográficamente aleatorias
   c) El hash del primer número generado mediante el generador pseudoaleatorio capaz de generar secuencias criptográficamente aleatorias
   d) Ninguna respuesta es correcta

12. Indique cuál de las siguientes afirmaciones es correcta:
    I. DES: algoritmo de cifrado en bloque, simétrico, con longitud de bloque 64 bits, con longitud de clave 64 bits, 16 iteraciones, 32 subclaves y proceso de descifrado idéntico al cifrado usando subclaves en orden inverso
    II. AES: algoritmo de cifrado en bloque, simétrico, con longitud de bloque 128/192/256 bits, con longitud de clave 128/192/256 bits, entre 10 y 14 iteraciones, número de subclaves en función del número de iteraciones y proceso de descifrado usando las inversas de las funciones empleadas para el cifrado y las subclaves en orden inverso
    a) I cierta, II cierta
    b) I cierta, II falsa
    c) I falsa, II cierta
    d) I falsa, II falsa

13. Indique cuál de las siguientes opciones es cierta:
    a) RC4 es un algoritmo de cifrado en flujo de clave simétrica
    b) RC4 es un algoritmo de cifrado en flujo de clave asimétrica
    c) RC4 es un algoritmo de cifrado en bloque de clave asimétrica
    d) RC4 es un algoritmo de cifrado en bloque de clave simétrica

14. Una vez inicializado el generador del algoritmo de cifrado de GSM, donde los polinomios característicos son (1) x^5+x^2+x+1, (2) $x+1$ y (3) $x^{15}+x^2+x+1$, y según el siguiente esquema, ¿cuál sería el valor de los dos siguientes bits de salida?

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
0	1	1	1	0	1	0	0	0	0	0	1	1	1	1	0	1	1	1

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
0	1	1	1	1	0	1	0	1	0	0	0	1	0	0	1	0	1	1	1	0	0

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22
1	1	1	0	0	0	1	0	1	1	0	1	0	0	1	1	0	0	1	1	1	0	1

    a) 1 1
    b) 1 0
    c) 0 1
    d) 0 0

15. El código MAC es
    a) La dirección física de la tarjeta de red de un PC
    b) Un bloque de bits de tamaño fijo obtenido a partir de un mensaje y una clave secreta
    c) Un bloque de bits de tamaño fijo obtenido a partir de un mensaje y una clave pública
    d) Ninguna respuesta es correcta

16. Indique cuál de las siguientes respuestas es correcta:
    I. La seguridad de HMAC depende en gran medida de la seguridad de la función hash que esté empleando
    II. Una implementación existente de una función hash se puede emplear como un módulo para implementar HMAC siempre que la longitud del *message digest* sea de al menos 128 bits
    a) I cierta, II cierta
    b) I cierta, II falsa
    c) I falsa, II cierta
    d) I falsa, II falsa

17. En los algoritmos de cifrado asimétrico:
    I. Es computacionalmente factible determinar la clave de descifrado si se conoce el algoritmo criptográfico y la clave de cifrado
    II. Podemos encontrar tres funcionalidades que son: proporcionar confidencialidad, proporcionar autenticación o permitir el intercambio de claves

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

18. Dada la clave e=5, los números primos p=19 y q=23, obtenga una clave pública válida para RSA:
a) d= 317
b) d= 437
c) d= 293
d) Ninguna respuesta es correcta

19. De los siguientes, indique cuál es el algoritmo de cifrado de voz empleado en GSM:
a) A3
b) A5
c) A8
d) COMP128

20. Si comparamos AES con 3DES, indique cuál de las siguientes opciones no es cierta:
a) En implementaciones software AES es del orden de tres veces más rápido que 3DES
b) AES y 3DES permiten tener diferentes longitudes de clave
c) AES es en general más seguro frente a un ataque por fuerza bruta que 3DES
d) Tanto AES como 3DES son métodos de cifrado convencional

21. Un sistema cortafuegos que examina los paquetes teniendo en cuenta a qué conexión pertenecen es:
a) Router filtrador de paquetes
b) Pasarela de aplicación
c) Cortafuegos de inspección de estado
d) Cortafuegos de zona desmilitarizada

22. Indique cuál de los siguientes protocolos permite crear redes privadas virtuales de capa 2:
a) SSH
b) IPSec
c) PPTP
d) Ninguna respuesta es correcta

23. Cuando un sistema tiene la característica de que la información sólo puede ser creada, modificada y destruida por los elementos del sistema autorizados para ellos, este sistema presenta:
a) Integridad
b) Confidencialidad
c) A) y b)
d) Ninguna respuesta es correcta

24. Una 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

25. ¿A qué se debe la relación teórica entre la longitud de las claves en RSA y en ECC para un mismo nivel de seguridad?
a) A que el problema de la factorización de enteros es más complejo (desde el punto de vista computacional) que el problema de los logaritmos discretos
b) A que el valor más pequeño de n (siendo n un número entero) para el cual nG=0 es un número primo grande (donde G es el punto generador de la curva elíptica)
c) A que es posible definir reglas de suma de los puntos que pertenecen a una curva elíptica, cumpliendo además las propiedades asociativa y conmutativa
d) Ninguna respuesta es correcta