ESCUELA TÉCNICA SUPERIOR DE INGENIERÍA DE TELECOMUNICACIÓN

DEPARTAMENTO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES

SEGURIDAD EN REDES DE COMUNICACIONES (4º curso, Grado de Ingeniería Telemática)

Examen Final. Fecha: 14 de febrero de 2014.

Alumno:														
Respuestas (A, B, C ó D)														
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40	41	42	43	44	45
46	47	48	49	50	51	52	53	54	55	56	57	58	59	60

Observaciones:

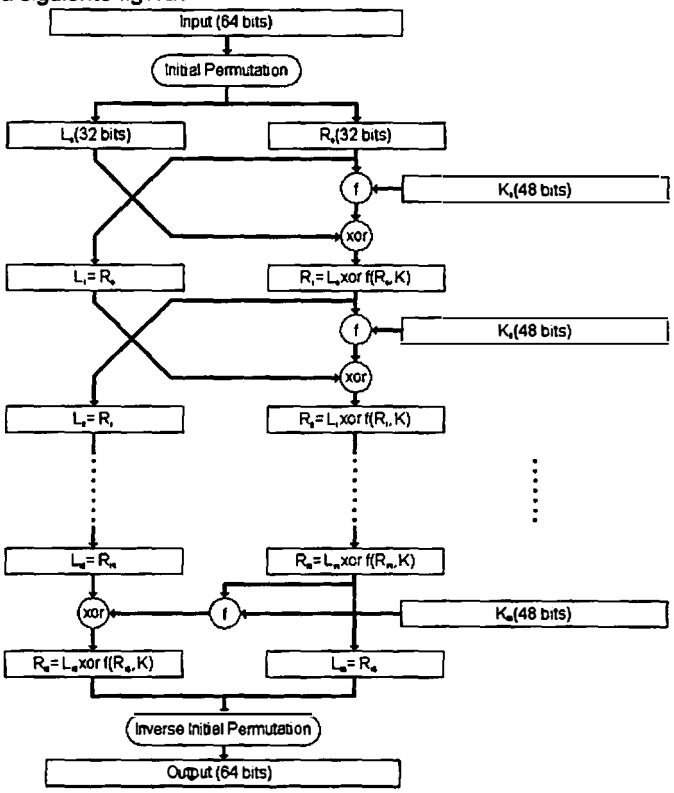
- Cada pregunta contestada correctamente sumará 1, cada respuesta incorrecta restará 1/3.
- Responder en la hoja de examen.

---

1. Qué operaciones de AES utilizan la tabla de estado [State] de tamaño 4x4:
   A) SubBytes
   B) ShiftRows
   C) AddRoundKey
   D) Todas son ciertas
2. Cuáles son caracterIsticas de AES:
   A) De dominio público, disponible para todo el mundo.
   B) Las claves de cifrado pueden ser de 128, 192 y 256 bits.
   C) Es implementable tanto en hardware como en software.
   D) Todas son ciertas
3. La función SubBytes:
   A) rota de manera cíclica los bytes en cada fila por un determinado offset
   B) actualiza cada byte usando la caja-S de Rijndael de 8 bits
   C) combina cuatro bytes de cada columna usando una transformación lineal inversible
   D) combina la subclave con el state
4. ¿Qué modo de cifrado DES trabaja como cifrador en bloque puro?
   A) Modo CBC (*Cipher Book Chaining*)
   B) Modo CFB (*Cipher feedback*)
   C) Modo OFB (*Output feedback*)
   D) Modo ECB (*Electronic code book*)
5. ¿Qué describe la siguiente ecuación (E y D cifradores DES): $Y = E_{K1}[D_{K2}[E_{K1}(X)]]$?
   A) Las demás son falsas
   B) Cifrador DES en modo ECB (*Electronic code book*)
   C) Cifrador 3DES en modo ECB (*Electronic code book*)
   D) Cifrador DES doble en modo ECB (*Electronic code book*)

6. ¿Cuál es la manera aconsejable usando clave asimétrica de garantizar confidencialidad y autenticación en un mensaje de A a B?
   A) $Y = E_{PB}[E_{PA}(X)]$
   B) $Y = E_{PA}[E_{PB}(X)]$
   C) $Y = E_{PB}[E_{PA}(X)]$
   D) $Y = E_{PA}[E_{PB}(X)]$

7. ¿Qué representa la siguiente figura?



   A) Ambas
   B) Un bloque cifrador DES usando las subclaves (de 48 bits) en secuencia K_1, K_2,... , K_{16}
   C) Un bloque descifrador DES usando las subclaves en secuencia K_{16}, K_{15}, ... , K_1
   D) Ninguna

8. ¿Cuál NO es un ingrediente necesario para RSA?
   A) Una e tal que d·e = n mod Φ(n)
   B) Números p y q primos, cuyo producto es n=p·q
   C) Φ(n)=(p-1)(q-1)
   D) Una d tal que el m.c.d. [Φ(n) , d] = 1 (1<d< Φ(n))

9. El algoritmo RSA deposita su confianza en:
   A) La intratabilidad del problema de la exponenciación modular
   B) La intratabilidad del problema del logaritmo discreto
   C) La intratabilidad del problema de hallar primos de más de 150 dígitos
   D) La intratabilidad del problema de la factorización

10. El algoritmo Diffie-Hellman deposita su confianza en:
   A) La desconfianza mutua Diffie-Hellman
   B) La dificultad de hallar una raíz primitiva de un número primo p
   C) La dificultad de calcular logaritmos discretos
   D) La dificultad de calcular la exponenciación discreta

11. Qué información NO debe viajar por el canal en un intercambio de claves Diffie-Hellman?
NOTA: $Y_a=\alpha^{Xa} \bmod q$ y $Y_b=\alpha^{Xb} \bmod q$
    A) Y_a y Y_b
    B) X_a y X_b
    C) α
    D) q
12. En curvas elípticas, la ecuación $(4 \cdot a^3 + 27 \cdot b^2) \bmod p \neq 0$ sirve para:
    A) Descartar elementos del grupo $E_p(a,b)$.
    B) Escoger las claves de cifrado a y descifrado b
    C) Eliminar el punto al infinito O del grupo
    D) Elegir la curva elíptica $E_p(a,b)$ sobre la que trabajar
13. Sabiendo que el punto P=(13,16) es un punto del grupo elíptico $E_{23}(1,1)$, ¿Qué punto Q será también del grupo?
    A) (13,7)
    B) (7,13)
    C) (10,16)
    D) Ninguno
14. Dado a=b=1 y p=23, con $y^2=x^3+ax+b \bmod p$, ¿qué 2 puntos se obtienen para x=3?
    A) (3,0) y (3,22)
    B) (3,10) y (3,13)
    C) (3,14) y (3,1)
    D) Ninguno
15. Un generador síncrono es aquél en el que:
    A) La secuencia es calculada de forma dependiente del texto plano e independiente del texto cifrado
    B) La secuencia es calculada de forma independiente del texto plano y dependiente del texto cifrado
    C) La secuencia es calculada de forma independiente tanto del texto plano como del texto cifrado
    D) La secuencia es calculada de forma dependiente tanto del texto plano como del texto cifrado
16. Sea la clave K1 una clave débil en DES. Esto significa que:
    A) no se puede cifrar X
    B) $D_{K1}(E_{K1}(X)) = X$
    C) $E_{K1}(D^{K1}(C)) = C$
    D) $E_{K1}(E_{K1}(X)) = X$
17. Indique cuál de las siguientes afirmaciones es cierta:
        I. En DES los datos se cifran en bloques de 64 bits.
        II. La longitud efectiva de la clave DES es de 56 bits.
    A) I cierta, II cierta,
    B) I cierta, II falsa
    C) I falsa, II cierta
    D) I falsa, II falsa
18. En relación con el tipo de amenazas y ataques que pueden sufrir los distintos elementos de una red de comunicaciones, diga cuál de las siguientes definiciones es verdadera:
    A) Un ataque se considera de interceptación cuando se ataca la integridad de un determinado objeto de la red de comunicación.
    B) Un ataque se considera de generación si consiste en una modificación del objeto original destinada a conseguir un objeto similar al atacado, de tal forma que éste sea difícilmente distinguible del original.
    C) Un ataque se considera de interrupción cuando se consigue el acceso a un determinado objeto de la red de comunicaciones.
    D) Un ataque se considera de modificación si el resultado es la pérdida del objeto atacado.
19. Una copia ilegal de una aplicación de correo electrónico es un ataque de:
    A) Interrupción
    B) Interceptación
    C) Generación
    D) Modificación

20. Indique cuál de las siguientes opciones es verdadera:
    A) El basureo es un ataque pasivo. Sin embargo, si la información que con él se obtiene, por ejemplo una clave de acceso, se utiliza para modificar el contenido de un fichero, entonces estaremos hablando de un ataque activo.
    B) Un ataque de suplantación es un ataque pasivo, mientras que un ataque de denegación de servicio es un ataque activo.
    C) Un ataque de suplantación es un ataque activo, mientras que un ataque de denegación de servicio es un ataque pasivo.
    D) Hacer uso de la utilidad whois para averiguar cuál es el espacio de direcciones IP asignado a una determinada compañía es un ataque activo.
21. El algoritmo de Diffie-Hellman se emplea básicamente para:
    A) Cifrar claves
    B) Autenticar claves
    C) Intercambiar claves
    D) Firmar claves
22. Si comparamos AES con 3DES, indique cuál de las siguientes opciones NO es cierta:
    A) Suponiendo AES y DES de igual velocidad, AES es 3 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.
23. En relación con el término Polltica de Seguridad, diga cuál de las siguientes opciones es FALSA:
    A) Previo a la elaboración de una Política de Seguridad es necesario llevar a cabo un análisis de riesgos.
    B) Una buena política de seguridad debe incluir un plan de contingencia.
    C) La política de seguridad no sólo debe incluir todos los objetivos de seguridad que se pretenden conseguir, sino que debe especificar las técnicas y mecanismos necesarios para alcanzarlos.
    D) Una buena política de seguridad debe definir claramente las áreas de responsabilidad de los usuarios, los administradores de la red y la dirección de la empresa.
24. Indique cuál de las siguientes opciones NO es cierta respecto a los algoritmos asimétricos de cifrado:
    A) Suelen ser más rápidos que los algoritmos de cifrado simétricos.
    B) Están basados en funciones matemáticas en vez de usar sustituciones o permutaciones
    C) Por lo general emplean longitudes de clave mucho mayores que los algoritmos de cifrado simétrico.
    D) En la práctica se emplean normalmente para cifrar la clave de sesión (simétrica) de cada mensaje o transacción particular
25. Dada la ecuación que define una curva elIptica $y2 \equiv x3+ax+b \pmod p$, donde a=b=1, y el número primo p = 19, ¿en qué cuadrante estarán los puntos del grupo elíptico Ep(a,b)?
    A) (1,1) a (19,19)
    B) (1,19) a (19,1)
    C) (0,0) a (1,1)
    D) Ninguna de las anteriores
26. Indique cuál de las siguientes opciones es FALSA. Previo al uso del Protocolo SET un usuario o comprador debe disponer de:
    A) Una clave simétrica de cifrado.
    B) Una cuenta en una entidad bancaria.
    C) Una tarjeta de crédito VISA o Mastercard.
    D) Un certificado X.509v3.
27. Según el algoritmo de Diffie-Hellman. Dado el número primo q=97 y un entero α=5 que es raíz primitiva de q. Si un usuario A escoge un valor secreto x_A=14 y un usuario B selecciona un valor secreto x_B=41, ¿cuál es la clave secreta que A y B conocen? [Precálculos: $5^{14} \bmod 97=48$; $5^{41} \bmod 97=80$; $41^{14} \bmod 97=86$; $80^{14} \bmod 97=66$]
    A) 48
    B) 80
    C) 86
    D) 66

28. ¿Cuál de las siguientes expresiones define la operación de cifrado y la de descifrado en RSA?
    A) $Y = X^n \log e$; $X = Y^n \log d$
    B) $Y = X^e \log n$; $X = Y^d \log n$
    C) $Y = X^n \bmod e$; $X = Y^n \bmod d$
    D) $Y = X^e \bmod n$; $X = Y^d \bmod n$
29. La principal ventaja de la criptografía de curva elíptica frente al algoritmo RSA es:
    A) Ofrece un nivel de confianza más alto que RSA ya que se viene estudiando desde hace décadas.
    B) Que sólo se emplea una única clave privada para cifrar y descifrar.
    C) Que ofrece la misma seguridad con longitudes de clave más pequeñas.
    D) Todas las anteriores.
30. En qué paso entra en funcionamiento el protocolo SET:
    1. Un cliente navega por la página WEB del vendedor.
    2. Decide comprar tres productos.
    3. Añade los productos a su carro de la compra.
    4. Rellena un formulario indicando su pedido y lo envía al vendedor.
    5. El vendedor le envía otro formulario en el que indica el precio total de la compra.
    6. El cliente verifica el pedido y envía al vendedor una orden de compra.
    7. El comerciante envía la petición de pago a su banco.
    8. El banco adquiriente valida al cliente al comerciante y obtiene una autorización de pago.....

    A) En el paso 1.
    B) En el paso 4.
    C) En el paso 6.
    D) En el paso 7.
31. El mecanismo conocido como firma DUAL dentro del protocolo SET consiste en:
    A) Asociar en un solo mensaje la orden de compra (OI) y la información de pago (PI). Dicho mensaje se obtiene calculando la función hash del resultado de concatenar los mensajes obtenidos de la aplicación de esa misma función hash tanto a la OI como a la PI.
    B) Usar dos firmas en cada certificado digital: (1) la de la autoridad de certificación reconocida por el banco del comprador y (2) la de la autoridad reconocida por el banco del vendedor.
    C) El vendedor dispone de dos certificados digitales: uno para firmar los mensajes que intercambia con el comprador y otro diferente para firmar los mensajes que intercambia con la pasarela de pagos.
    D) El vendedor dispone de un único certificado que le permite firmar los mensajes que intercambia con el comprador y con la pasarela de pagos.
32. Indique cuál de las siguientes opciones es cierta:
    A) RC4 es un algoritmo de cifrado en bloque de clave asimétrica
    B) RC4 es un algoritmo de cifrado en bloque de clave simétrica
    C) RC4 es un algoritmo de cifrado en flujo de clave simétrica
    D) RC4 es un algoritmo de cifrado en flujo de clave asimétrica
33. El protocolo que se encarga de garantizar la confidencialidad de los datos dentro del conjunto de protocolos de SSL es:
    A) El protocolo SSL Record
    B) El protocolo SSL Handshake
    C) El protocolo SSL Alert
    D) El protocolo SSL Change Session-Spec
34. Indique cuál de las siguientes opciones es falsa:
    A) SHA-1 es más fuerte frente a ataques por fuerza bruta
    B) Tanto SHA-1 como MD5 funcionan bien en arquitecturas de 32 bits
    C) MD5 genera un bloque de 128 bits y SHA-1 genera un bloque de 160 bits
    D) En el mismo hardware SHA-1 es más rápido que MD5

35. Indique cuál de las siguientes opciones es cierta:
    I. RC4 es básicamente un generador de números pseudo-aleatorios inicializados con una clave secreta típicamente entre 40 y 256 bits.
    II. Uno de los motivos de la popularidad de RC4 es su sencilla implementación software.
    A) I cierta, II cierta
    B) I cierta, II falsa
    C) I falsa, II cierta
    D) I falsa, II falsa
36. De los siguientes, indique cuál es el algoritmo de autenticación de la SIM ante una red GSM:
    A) A3
    B) A5
    C) A8
    D) COMP128
37. En el protocolo SSL se usa una clave de sesión para cifrar la información. Esta clave…
    A) Es la clave privada del cliente.
    B) Es la clave pública del cliente.
    C) Es una clave común, generada en ambos extremos independientemente, mediante la información intercambiada durante el protocolo de SSL Handshake.
    D) Es una clave común, generada por el cliente, cifrada con la clave pública del servidor y enviada al servidor.
38. Las técnicas de autenticación evitan ataques del tipo:
    A) Enmascaramiento
    B) Modificación de la secuencia
    C) Modificación de contenidos
    D) Todos los anteriores
39. Indique cuál de las siguientes opciones es FALSA. Los objetivos del protocolo SSL Handshake son:
    A) Llegar a un acuerdo entre cliente y servidor sobre qué versión utilizar.
    B) Elegir el tipo de alertas que el cliente puede enviar: sólo alertas fatales o alertas fatales y avisos.
    C) Elegir el método de compresión de datos utilizado.
    D) Elegir una determinada suite de cifrado.
40. Indique cuál de las siguientes afirmaciones es cierta:
    A) El cifrado simétrico ofrece confidencialidad y autenticación
    B) El cifrado asimétrico ofrece confidencialidad y autenticación
    C) El cifrado simétrico ofrece confidencialidad pero no autenticación
    D) Todas las anteriores son falsas
41. La cadena E7BA ECB5 2A9F DDEB 9BC8 CEA8 8B0A 1A69 ABCD 1234 podría ser un:
    A) hash MD5
    B) hash SHA-1
    C) bloque cifrado 3DES
    D) bloque cifrado DES
42. Indique cuál de las siguientes opciones es cierta:
    I. La seguridad de HMAC depende de la función hash empleada.
    II. Cualquier función hash existente se puede emplear como un módulo dentro de HMAC.
    A) I cierta, II cierta
    B) I cierta, II falsa
    C) I falsa, II cierta
    D) I falsa, II falsa
43. Indique cuál de las siguientes opciones es FALSA:
    A) El proceso de descifrado en DES es básicamente el mismo que el de cifrado, la única diferencia es que se usan las subclaves en orden inverso
    B) El algoritmo DES es un proceso iterativo que consta de 20 rondas o iteraciones
    C) Uno de los posibles puntos débiles de DES es su escasa longitud de clave
    D) DES ofrece cuatro modos de funcionamiento: ECB, CBC, CFB y OFB

44. Suponga que accede a su banco online. Nada más abrir la página aparece un mensaje como que está accediendo a un servidor web seguro. Si usted la única operación que ha realizado ha sido abrir la página, ¿cómo puede saber que realmente está accediendo a un sitio seguro?
    A) Porque dispongo de un certificado personal
    B) Porque tras instalar el navegador me puse en contacto con las autoridades certificadoras para que éstas me enviaran sus claves públicas, pudiendo así comprobar su veracidad
    C) Porque normalmente el navegador dispone de la clave pública de la autoridad certificadora que emite el certificado, pudiendo así comprobar su veracidad
    D) No lo puedo saber a ciencia cierta, he de confiar en la entidad bancaria
45. En terminología Kerberos un dominio de administración es:
    A) Un principal
    B) Un reino
    C) Un principado
    D) Un billete
46. ¿Por qué es mejor utilizar el protocolo de seguridad ESP frente al protocolo de seguridad AH, cuando se crea una red privada virtual basada en IPSec?
    A) ESP proporciona un servicio contra el reenvío de paquetes y AH no.
    B) ESP proporciona integridad de datos y AH no.
    C) ESP proporciona confidencialidad y AH no.
    D) ESP proporciona autenticación del origen de los datos y AH no.
47. La misión del servidor de autenticación (AS) de Kerberos es:
    A) Enviar al cliente una clave de sesión
    B) Emitir un TGT
    C) Comprobar que el usuario del servicio esté incluido en la base de datos del KDC
    D) Todas las anteriores
48. Indique cuál de las siguientes opciones NO es cierta respecto a las limitaciones de Kerberos v.4:
    A) Sólo se emplea DES para el cifrado de mensajes
    B) Requiere el uso de direcciones IP
    C) El tiempo de vida máximo de un billete es bastante limitado
    D) No es posible la autenticación entre diferentes dominios administrativos de Kerberos
49. Triple DES es un algoritmo de cifrado/descifrado que emplea:
    A) Una clave
    B) Dos claves
    C) Tres claves
    D) Cuatro claves
50. ¿El campo SPI de la cabecera ESP se cifra?
    A) No, porque sin el valor del campo SPI no es posible determinar que asociación de seguridad se está utilizando y, en consecuencia, no se podría saber que clave utilizar para descifrar los datos.
    B) Sí, el parámetro SPI se cifra, al igual que el resto de la trama ESP.
    C) No, porque su valor es el valor asignado al protocolo ESP y, por tanto, se trata de un valor conocido que no hace falta proteger.
    D) No, porque el protocolo ESP no proporciona un servicio de confidencialidad.
51. Indique cuál de las siguientes afirmaciones es FALSA en EAP:
    A) El tipo NAK sólo es válido en los paquetes response
    B) El tipo NAK se envía cuando el tipo de autenticación requerida es inaceptable
    C) Las implementaciones de EAP PPP sólo deben soporta obligatoriamente los tipos: Identity, Notification, NAK y MD5 challenge
    D) Si el autenticador no puede autenticar al otro extremo le enviará un paquete EAP del tipo Notification
52. Con Kerberos, para que un usuario pueda acceder a u servicio debe tener:
    A) un código hash
    B) un certificado X.500
    C) un billete
    D) un código HMAC

53. Indique cuál de los siguientes datos es necesario para identificar de forma única una asociación de seguridad:
    A) La dirección IP destino
    B) El valor del campo SPI de las cabeceras IPSec (ESP o AH)
    C) El protocolo IPSec que se está utilizando (ESP o AH)
    D) Todas son ciertas
54. ¿Cuál de los siguientes NO es un campo incluido en el estándar más popular hoy en día que define un marco para la provisión de servicios de autenticación mediante certificados?
    A) Versión
    B) nombre del emisor del certificado
    C) información de la clave privada del sujeto
    D) identificador del algoritmo de firma
55. El intercambio de autenticación en 802.1x se realiza entre:
    A) Suplicante y servidor de autenticación
    B) Suplicante y autenticador
    C) Usuario y suplicante
    D) Usuario y autenticador
56. Indique cuál de las siguientes opciones NO es una limitación de IPSec:
    A) IPSec no soporta tráfico multicast o broadcast.
    B) IPSec no permite la creación de túneles punto-multipunto.
    C) IPSec no se puede utilizar para encapsular protocolos distintos de IP (IPv4 e IPv6), como por ejemplo IPX o Apple Talk.
    D) No es posible usar NAT e IPSec al mismo tiempo.
57. Un certificado sirve para:
    A) Verificar la clave privada de un usuario.
    B) Verificar la clave pública de un usuario
    C) a) y b)
    D) Ninguna de las anteriores
58. En relación con los modos de funcionamiento de los protocolos IPSEC, indique cuál de las siguientes opciones es verdadera:
    A) El protocolo AH tiene un solo modo de funcionamiento: modo transporte.
    B) El protocolo ESP tiene un solo modo de funcionamiento: modo túnel.
    C) El modo transporte sólo se puede utilizar para establecer asociaciones de seguridad entre dos hosts (o dos máquinas que actúan como tales).
    D) El modo túnel sólo se puede utilizar entre dos pasarelas de seguridad.
59. ¿Cuál es el estándar más popular hoy en día que define un marco para la provisión de servicios de autenticación mediante certificados?
    A) X.608
    B) X.802
    C) X.509
    D) X.500
60. La generación de subclaves en AES 128 consiste en a partir de una clave inicial de 128 bits generar claves de 128 bits para 10 rondas mediante operaciones RotWord, SubBytes, Rcon y XOR. Esto se hace:
    A) Bloque a bloque, cada subclave de 128 bits se obtiene haciendo RotWord, SubBytes, Rcon y XOR, de manera independiente de las demás.
    B) Cada subclave depende de la anterior, repitiendo las mismas operaciones RotWord, SubBytes, Rcon y XOR para cada subclave.
    C) Se usa la misma clave para cada ronda.
    D) Para la primera, segunda y tercera subclave se usa RotWord, cuarta, quinta y sexta SubBytes, séptima, octava y novena Rcon, décima XOR.