ESCUELA TÉCNICA SUPERIOR DE INGENIERÍA DE TELECOMUNICACIÓN

DEPARTAMENTO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES

SEGURIDAD EN REDES DE COMUNICACIONES (Ingeniero de Telecomunicación)

Alumno: _____

Observaciones: *Cada pregunta contestada correctamente sumará 1, cada respuesta incorrecta restará 1/3.*

---

1. Encontramos que la clave K_1 es débil en DES. Esto significa que:

A) $E_{k1}(E_{K1}(X)) = X$

B) no se puede cifrar X

C) $D_{k1}(E_{K1}(X)) = X$

D) $E_{k1}(D_{K1}(C)) = C$

2. Indique cuál de las siguientes afirmaciones es cierta:

I. En DES los datos se cifran en bloques de 64 bits.

II. La longitud 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

3. 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 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.

B) Un ataque se considera de interrupción cuando se consigue el acceso a un determinado objeto de la red de comunicaciones.

C) Un ataque se considera de modificación si el resultado es la pérdida del objeto atacado.

D) Un ataque se considera de interceptación cuando se ataca la integridad de un determinado objeto de la red de comunicación.

4. Una copia ilegal de una aplicación de correo electrónico es un ataque de:

A) Interceptación

B) Interrupción

C) Generación

C) Modificación

5. ¿Cuál de las siguientes afirmaciones NO es cierta sobre AES?

A) AES es un sistema de cifrado simétrico

B) AES permite utilizar diferentes longitudes de clave

C) AES realiza las operaciones internas a nivel de palabras de 16 bits

D) AES es un sistema de cifrado basado en rondas o iteraciones

6. Indique cuál de las siguientes opciones es verdadera:

A) Un ataque de suplantación es un ataque pasivo, mientras que un ataque de denegación de servicio es un ataque activo.

B) Un ataque de suplantación es un ataque activo, mientras que un ataque de denegación de servicio es un ataque pasivo.

C) 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.

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.

7. El algoritmo de Diffie-Hellman se emplea básicamente para:

A) cifrar

B) autenticar

C) intercambiar claves

D) ninguna de las anteriores

8. 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.

9. En relación con el término Política 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) 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.

C) Una buena política de seguridad debe incluir un plan de contingencia.

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.

10. Indique cuál de las siguientes opciones NO es cierta respecto a los algoritmos asimétricos de cifrado:

A) están basados en funciones matemáticas en vez de usar sustituciones o permutaciones

B) por lo general emplean longitudes de clave mucho mayores que los algoritmos de cifrado simétrico

C) suelen ser más rápidos que los algoritmos de cifrado simétricos

D) en la práctica se emplean normalmente para cifrar la clave de sesión (simétrica) de cada mensaje o transacción particular

11. Dada la ecuación que define una curva elíptica $y^2 \equiv x^3+ax+b \pmod p$, donde a=b=1, y el número primo p = 23, ¿en qué cuadrante estarán los puntos del grupo elíptico $E_p(a,b)$?

A) (1,1) a (23,23)

B) (1,23) a (23,1)

C) (0,0) a (1,1)

D) ninguno de los anteriores

12. Indique cuál de las siguientes opciones es FALSA. Previo al uso del Protocolo SET un usuario o comprador debe disponer de:

A) Una cuenta en una entidad bancaria.

B) Una tarjeta de crédito VISA o Mastercard.

C) Una clave simétrica de cifrado.

D) Un certificado X.509v3.

13. Si en AES se utiliza un tamaño de bloque de 192 bits, ¿cuál es el tamaño de la matriz de estado?

A) 4x4

B) 4x6

C) 6x4

D) 8x4

14. 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=26 y un usuario B selecciona un valor secreto x_B=40, ¿cuál es la clave secreta que A y B conocen?

A) 62

B) 60

C) 61

D) 59

15. ¿Cuál de las siguientes expresiones define la operación de cifrado y la de descifrado en RSA?

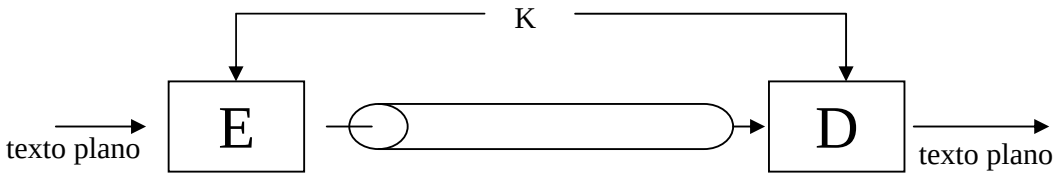
A) $Y = X^n \log e$; $X = Y^n \log d$

B) $Y = X^e \log n$; $X = Y^d \log n$

C) $Y = X^n \bmod e$; $X = Y^n \bmod d$

D) $Y = X^e \bmod n$; $X = Y^d \bmod n$

16. El siguiente esquema se corresponde con



A) cifrado en flujo

B) cifrado simétrico

C) cifrado en bloque

D) cifrado asimétrico

17. La principal ventaja de la criptografía de curva elíptica frente al algoritmo RSA es:

A) que ofrece un nivel de confianza más alto que RSA ya que se viene estudiando desde hace décadas

B) que ofrece la misma seguridad con longitudes de clave más pequeñas

C) que sólo se emplea una única clave privada para cifrar y descifrar

D) todas las anteriores

18. 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.....

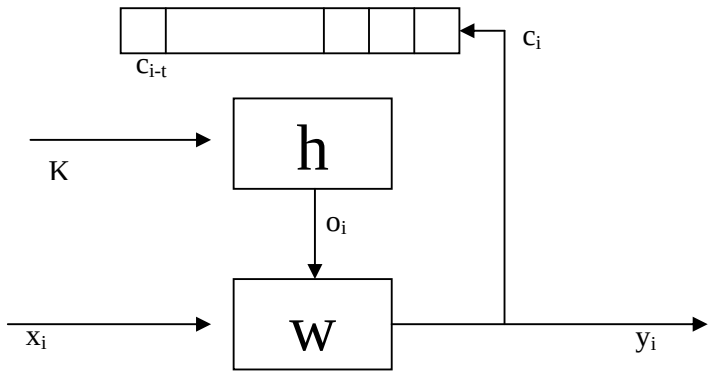
A) En el paso 7.

B) En el paso 6.

C) En el paso 1.

D) En el paso 4.

19. ¿Qué tipo de generador de secuencias muestra la siguiente figura?



A) Generador síncrono

B) Generador asíncrono

C) Generador secuencial

D) Ninguna de las anteriores

20. El mecanismo conocido como firma DUAL dentro del protocolo SET consiste en:

A) 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.

B) 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.

C) El vendedor dispone de un único certificado que le permite firmar los mensajes que intercambia con el comprador y con la pasarela de pagos.

D) 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.

21. 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

22. 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*

23. Indique cuál de las siguientes opciones es cierta:

I. El protocolo IEEE 802.1x no se puede utilizar en entornos inalámbricos.

II. El protocolo IEEE 802.1x se puede utilizar para el intercambio de claves de cifrado.

A) I cierta, II cierta

B) I cierta, II falsa

C) I falsa, II cierta

D) I falsa, II falsa

24. 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) De momento no se conocen ataques por criptoanálisis a SHA-1

D) En el mismo *hardware* SHA-1 es más rápido que MD5

25. Indique cuál de las siguientes opciones es cierta:

I. RC4 es básicamente un generador de números pseudo-aleatorios inicializados con una clave secreta de hasta 40 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

26. De los siguientes, indique cuál es el algoritmo de cifrado de voz empleado en GSM:

A) A3

B) A5

C) A8

D) COMP128

27. En el protocolo SSL se usa una clave de sesión para cifrar la información. Esta clave…

A) Es la clave privada del cliente.

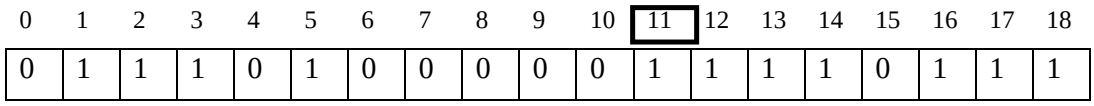
B) Es la clave pública del cliente.

C) Es una clave común, generada en ambos extremos independientemente, mediante la información intercambiada durante el protocolo de SSL *Handshake*.

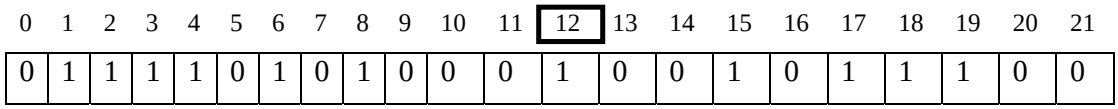
D) Es una clave común, generada por el cliente, cifrada con la clave pública del servidor y enviada al servidor.

28. Una vez inicializado el generador del algoritmo de cifrado de voz de GSM, donde los polinomios característicos son (1) x^5+x^2+x+1, (2) $x+1$ y (3) $x^{15}+x2+x+1$, y según el siguiente esquema, ¿cuál sería el valor de los dos siguientes bits de salida?

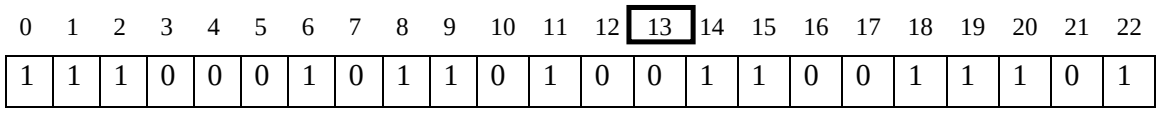
SALIDA



(1)



(2)



(3)

A) 1 1

B) 1 0

C) 0 1

D) 0 0

29. Las técnicas de autenticación evitan ataques del tipo:

A) enmascaramiento

B) modificación de la secuencia

C) modificación de contenidos

D) todos los anteriores

30. 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.

31. 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

32. La cadena E7BA ECB5 2A9F DDEB 9BC8 CEA8 8B0A 1A68 podría ser un

A) *hash* MD5

B) *hash* SHA-1

C) bloque cifrado 3DES

D) bloque cifrado DES

33. Indique cuál de las siguientes opciones es cierta:

I. La seguridad de HMAC es independiente 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

34. Indique cuál es el orden seguido por el protocolo PGP, para proporcionar los servicios de autenticación, confidencialidad, compresión de datos y conversión a RADIX64 (se ha indicado sólo la parte correspondiente al emisor):

A) En primer lugar, se comprime el mensaje que se va a enviar. A continuación se calcula el *hash* del mensaje comprimido. El *hash* se firma y se concatena con el mensaje comprimido. El conjunto se cifra con la clave de sesión y se convierte a RADIX 64.

B) En primer lugar se calcula el *hash* del mensaje a transmitir. El *hash* se firma y se concatena al mensaje original. El resultado se comprime y, a continuación, se cifra con la clave de sesión. Por último, el resultado se convierte a RADIX 64.

C) En primer lugar se convierte el mensaje a RADIX 64, a continuación se comprime y se firma usando la clave de sesión. Por último se cifra utilizando una vez más la clave de sesión.

D) En primer lugar se calcula el *hash* del mensaje a transmitir. El *hash* se firma y se concatena al mensaje original. A continuación se cifra con la clave de sesión y se convierte a RADIX 64. Por último, el resultado se comprime.

35. 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

36. 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

37. En terminología Kerberos un dominio de administración es:

A) un principal

B) un reino

C) un principado

D) una realización

38. Cuál es el objetivo de la conversión RADIX 64 utilizada en PGP:

A) Incrementar la tasa de compresión los mensajes cifrados.

B) Añadir una protección adicional a la integridad de los datos protegidos.

C) Adaptar los caracteres del mensaje cifrado para que sean compatibles con todos los servidores de correos.

D) Convertir las claves de sesión cortas en claves con una longitud de al menos 64 bits.

39. En un intercambio de mensajes en 802.1x (en red cableada) en el que no se producen errores, ¿cuántos mensajes circularían por la red?

A) siete

B) ocho

C) nueve

D) diez

40. ¿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.

41. 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 que quiere acceder al servicio está incluido en la base de datos del KDC

D) Todas las anteriores

42. En una comunicación normal con Kerberos versión 4 dentro de un mismo dominio se emplean _____ claves mientras que con Kerberos versión 5 se emplean _____ claves

A) dos, cuatro

B) tres, cinco

C) cuatro, cuatro

D) cinco, cinco

43. ¿Cuál de los siguientes protocolos proporciona un servicio de autenticación del origen de los datos?

A) IKE

B) ESP en modo transporte

C) AH

D) RSA

44. 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

45. Indique cuál de las siguientes opciones es FALSA:

A) El protocolo EAP PPP soporta múltiples mecanismos de autenticación

B) Con el protocolo EAP PPP podemos emplear un servidor de autenticación que realmente implemente los mecanismos de autenticación, dejando al autenticador sólo para intercambiar mensajes

C) El paquete PPP se encapsula dentro del campo datos del paquete EAP PPP

D) El formato del paquete EAP PPP es: código, identificador, longitud y datos.

46. Triple DES es un algoritmo de cifrado/descifrado que emplea:

A) Una clave

B) Dos claves

C) Tres claves

D) Cuatro claves

47. ¿Por qué el campo SPI de la cabecera ESP no se cifra?

A) 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) El parámetro SPI sí que se cifra.

C) Porque su valor es el valor asignado al protocolo ESP y, por tanto, se trata de un valor conocido que no hace falta proteger, y que se podría utilizar para descifrar el resto del mensaje.

D) Porque el protocolo ESP no proporciona un servicio de confidencialidad.

48. Indique cuál de las siguientes afirmaciones es FALSA:

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*

49. 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

50. Indique cuál de los siguientes datos NO 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) La dirección IP origen

51. ¿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

52. 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

53. Indique cuál de las siguientes opciones NO es una limitación de IPSec:

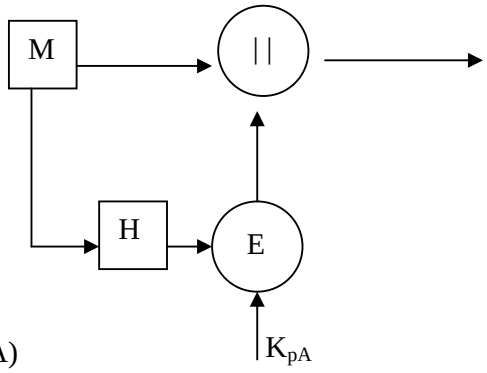
A) IPSec no soporta tráfico *multicast* o *broadcast*.

B) IPSec no permite la creación de túneles punto-multipunto.

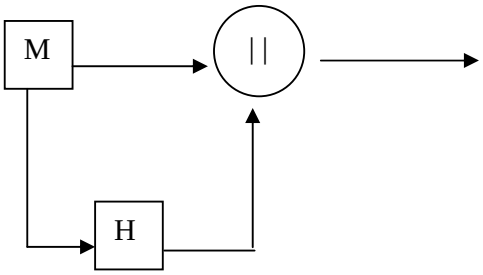
C) IPSec no se puede utilizar para encapsular protocolos distintos de IP (IPv4 e IPv6), como por ejemplo IPX o Apple Talk.

D) No es posible usar NAT e IPSec al mismo tiempo.

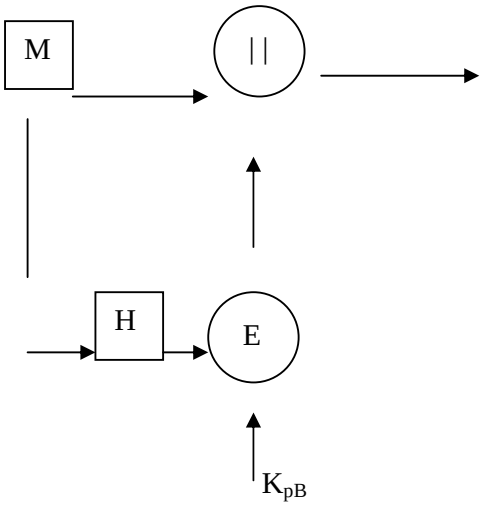
54. Indique con cuál de los siguientes esquemas el usuario A estará incluyendo una firma digital para el mensaje M:



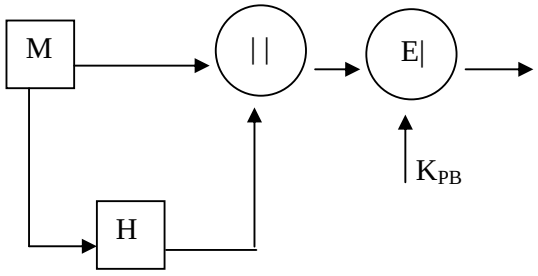
A)



B)



C)



D)

55. 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

56. 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.

57. Imagine que usted dispone de un certificado personal y detecta que alguien ha violado la privacidad de su ordenador, comprometiendo así la seguridad de su clave privada. ¿Qué debe hacer?:

A) Informar a la autoridad certificadora para que revoque el certificado

B) Cambiar la clave secreta para evitar que otra persona pueda suplantar mi identidad

C) Solicitar a la autoridad certificadora otra clave privada

D) Nada, puesto que aunque alguien conozca mi clave privada no puede suplantar mi identidad

58. ¿Qué es una CGA (*Criptographic Generated Address*)?

A) Una dirección IP de una interfaz IPv6 generada aplicando una función resumen a la clave pública del propietario de la misma.

B) Una dirección IP de una interfaz IPv6 generada aplicando una función resumen a la clave privada del propietario de la misma.

C) Una dirección IP de una interfaz IPv4 generada aplicando una función resumen a la clave pública del propietario de la misma.

D) Una dirección IP de una interfaz IPv6 que sustituye a la dirección IP original de la interfaz, y que se obtiene cifrando dicha dirección con una clave simétrica compartida entre los miembros de una red de comunicaciones.

59. ¿Cuál de los siguientes no es un tipo de certificado digital?

A) certificado de *hardware*

B) certificado de autoridad certificadora

C) certificado personal

D) certificado de servidores

60. ¿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