Test Tema 79 #1

Actualizado el 13/04/2025

1. El algoritmo de cifrado Rijndael:

a) Compite con AES por ser el estándar de criptografía dominante
b) Es un algoritmo de clave pública
c) Es un desarrollo propietario de IBM
d) Se basa en la teoría de campos de Galois

2. Señale qué módulo criptográfico debe tener instalado un ordenador para que el usuario pueda utilizar el DNI electrónico:

a) No es necesario ningún módulo criptográfico.
b) Debe estar instalado "Cryptographic Service Provider" (CSP) o el módulo PKCS#11 indistintamente.
c) En los entornos UNIX / Linux o MAC debe estar instalado el módulo PKCS#11.
d) En un entorno Microsoft Windows debe estar instalado el módulo PKCS#11.

3. Mediante la emisión de un sello de tiempo sobre un documento:

a) se puede demostrar que el contenido del documento es correcto.
b) se generará una evidencia, que determinará la existencia de ese documento en un instante determinado.
c) se puede garantizar la fecha y la hora en la que se creó el documento.
d) se asegura la fecha y la hora de la sede electrónica.

4. PGP son una siglas muy conocidas dentro del mundo del cifrado y de la seguridad. ¿A qué corresponden?

a) Pretty Good Privacy
b) Personal General Privacity
c) Privacity Generator Program
d) Ninguna de las anteriores respuestas es correcta

5. ¿Qué tecnología sustituyó a DES tras su ruptura?

a) Rijndael
b) RC-4
c) MD5
d) SEAL

6. El ganador del concurso público para reemplazar al algoritmo DES es:

a) RC6
b) Twofish
c) Serpent
d) Rijndael

7. En los algoritmos de clave simétrica:

a) se pueden distribuir y mantener fácilmente las claves
b) tienen alta velocidad de cifrado y descifrado
c) no se ha alcanzado aún la perfección matemática, y existen algoritmos eficaces para reventarlos aparte del de fuerza bruta
d) no pueden ser usados para autenticar a las partes

8. La ciencia que trata de descifrar mensajes cifrados sin conocer los códigos se denomina:

a) Criptoanálisis o análisis criptográfico
b) Ingeniería social
c) Fuerza Bruta
d) Criptografía

9. ¿Cuál de los siguientes NO es un modo de operación del algoritmo de cifrado DES (Data Encryption Standard)?

a) Modo ECB (Electronic Code Book Mode).

b) Modo CFB (Cipher Feedback Mode).

c) Modo BBM (Bit Block Mode).

d) Modo CBC (Cipher Block Chaining Mode).

10. Si un intruso intenta cotillear (eavesdropping) durante el proceso de generación de las claves generadas por criptografía cuántica:

a) El sistema lo rechaza

b) Las claves generadas se ven alteradas y se descubre el intento de intrusión

c) Al intentar usar las claves interceptadas le propone el sistema un challenge o desafío adicional

d) Sólo puede hacerlo si se usan cifradores de flujo

11. Cuál es el uso más generalizado de las funciones irreversibles tipo HASH:

a) Para cifrar y descifrar mensajes

b) Para firma electrónica

c) Para garantizar la confidencialidad

d) Para encriptar mensajes

12. ¿Qué es Kleopatra?

a) El equivalente en Android al servicio Kerberos de Windows

b) Una aplicación de gestión criptográfica basada en GPG

c) Un navegador del entorno KDE

d) La última versión de Debian

13. ¿Cuál de los siguientes sistemas de cifrado permite comprobar la identidad de los interlocutores y asegurar la confidencialidad del mensaje?

a) SHA-2

b) RSA

c) AES

d) DES

14. ¿Qué es la esteganografía?

a) Es una técnica que busca ocultar un mensaje ante un posible atacante cifrando dicho mensaje.

b) Es una técnica que consiste en cambiar el orden de los símbolos.

c) Es una técnica que consiste en sustituir un símbolo por otro de un conjunto.

d) Es una técnica que busca ocultar un mensaje ante un posible atacante haciendo que pase desapercibido.

15. ¿Cuál de los siguientes sistemas de cifrado no es una alternativa aceptable para DES (Data Encryption Standard)?

a) RC-4

b) IDEA

c) Triple DES

d) RSA

16. En la criptografía de clave pública, si queremos garantizar la autenticidad y el no repudio en origen de un mensaje que enviamos a un tercero, ¿con qué clave debemos cifrar nuestro mensaje?

a) Con nuestra clave pública.

b) Con nuestra clave privada.

c) Con la clave pública del receptor.

d) Con la clave privada del receptor.

17. El algoritmo DES:

a) Es un algoritmo de cifrado asimétrico que codifica bloques de 64 bits empleando claves de 32 bits, con una permutación al principio y otra al final del proceso.

b) Es un algoritmo de cifrado por bloques que codifica bloques de 54 bits, y su estructura consta de 16 etapas.

c) Es un algoritmo de cifrado simétrico cuya estructura es una variación de la red de Feistel.

d) Es un algoritmo de cifrado de flujo que codifica flujos de 64 bits, empleando una clave de 64, aunque sólo 56 bits son utilizados. Los 8 bits restantes comprueban la paridad.

18. Indique cuál de las siguientes afirmaciones es correcta:

a) En un sistema de cifrado de clave asimétrica la seguridad radica en la transmisión de la clave, mediante canal seguro, entre el emisor y el receptor del mensaje.

b) Las huellas digitales devueltas por una misma función hash tienen idéntica longitud.

c) Para ofrecer un nivel de seguridad equivalente, los sistemas de clave pública requieren menores longitudes de clave que los sistemas simétricos.

d) Se denomina criptograma al procedimiento empleado para cifrar un mensaje.

19. Señale la opción INCORRECTA respecto a sistemas criptográficos:

a) En un sistema de cifrado de clave asimétrica, la seguridad radica en la transmisión de la clave mediante canal seguro entre el emisor y el receptor del mensaje

b) La criptografía asimétrica incluye sistemas basados en factorización entera, el problema del logaritmo discreto y el problema del logaritmo discreto elíptico

c) La criptografía asimétrica se fundamenta en la imposibilidad práctica de resolver ciertos problemas matemáticos de forma eficiente

d) Dos de las aplicaciones principales de la criptografía de clave pública son el intercambio seguro de claves privadas y la firma digital

20. Comparando la criptografía de clave secreta frente a la criptografía asimétrica. ¿Cuál de los dos tipos de criptografía es más segura, suponiendo igual longitud de clave?

a) La de clave secreta

b) La asimétrica

c) Son igual de seguras

d) Depende del lenguaje de programación empleado

21. Indique cuál de los siguientes algoritmos criptográficos se basa en el logaritmo discreto elíptico:

a) RSA

b) RW

c) Diffie-Hellman

d) DSAE

22. La técnica criptográfica basada en un conjunto de métodos que permiten tener comunicación segura entre las partes, siempre y cuando previamente ambas partes hayan intercambiado una clave privada, se denomina:

a) Criptografía asimétrica.

b) Criptografía simétrica.

c) Criptografía de clave pública.

d) Criptografía paralela.

23. La captura de los datos de una tarjeta de crédito por un tercero, en una transacción económica realizada a través de internet entre un comprador y una tienda de comercio electrónico afecta a:

a) La dimensión de integridad de la información en tránsito

b) La dimensión de autenticación del destinatario de la información en tránsito

c) La dimensión de confidencialidad de la información en tránsito

d) La dimensión de disponibilidad de la información en tránsito

24. Sobre el algoritmo de cifrado RSA en no es cierto que:

a) Es utilizado para firmar digitalmente
b) Fue propuesto por Diffie y Hellman
c) Lo que se cifra con la clave privada se descifra con la pública
d) Lo que se cifra con la clave pública se descifra con la privada

25. Camellia es un algoritmo:

a) Simétrico de bloque
b) Simétrico de flujo
c) Asimétrico
d) De función hash

26. El algoritmo RSA es un algoritmo:

a) De triple clave.
b) Asimétrico.
c) De clave privada.
d) Simétrico.

27. ¿Cuál es un algoritmo de criptografía simétrica de flujo?

a) DES
b) Blowfish
c) SNOW
d) IDEA

28. ¿Con qué campo de la informática se relaciona SHA-2?

a) Data Mining
b) La Criptografía
c) El e-learning
d) La gestión de versiones

29. Indique cuál de los siguientes algoritmos utiliza cifrado de clave pública:

a) Rigndael
b) RSA
c) 3DES
d) Blowfish

30. El algoritmo RSA se emplea para:

a) Cifrar datos con una clave secreta
b) Cifrar datos con una criptografía de clave pública
c) Obtener un resumen (huella digital) de un documento
d) Ninguna de las anteriores

31. Los algoritmos de cifrado que utilizaban los antiguos romanos eran de clave:

a) simétrica
b) asimétrica
c) diferencial
d) clave simétrica o asimétrica, dependiendo del algoritmo

32. ¿Cuál de las siguientes no corresponde a una función digest?

a) HMAC
b) MD5
c) MD8
d) SHA

33. Los cifrados de clave pública:

a) De Diffie-Hellman basan su fortaleza en la dificultad de resolver el problema de los logaritmos discretos

b) A igualdad de longitud de clave los basados en curvas elípticas son tan robustos como los basados en la aritmética modular

c) La llegada de los ordenadores cuánticos no los hará más vulnerables a los métodos criptoanalíticos empleados ahora

d) Basados en el RSA requieren más tiempo para descifrar que para generar sus pares de claves

34. Dado un mensaje, m, y su cifrado mediante OTP (one time pad), c ¿se puede obtener la clave utilizada en el cifrado?

a) No, no se puede
b) Sí, la clave es k = m XOR c
c) Sólo pueden calcularse la mitad de los bits de la clave
d) Sí, la clave es k = m XOR m

35. Respecto al algoritmo RSA:

a) Reduce el problema de la distribución de claves respecto a los criptosistemas clásicos
b) Pertenece a la categoría de criptosistemas simétricos
c) Se basa en la utilización de grandes series de números primos de tamaño pequeño
d) Se basa en la transposición y sustitución de símbolos a través de múltiples iteraciones

36. ¿Cuál de los siguientes algoritmos no sirve de base para la definición de algoritmos de criptografía asimétrica?

a) Problema de sustitución afín
b) Problema de factorización entera
c) Problema de logaritmo discreto
d) Problema de logaritmo discreto elíptico

37. Indicar la respuesta falsa:

a) IDEA es un algoritmo de clave simétrica
b) RIPMED utiliza claves de 128 bits
c) SHA-1 utiliza claves de 160 bits
d) La seguridad de una función hash radica en su carácter unidireccional

38. La afirmación: "La factorización de números enteros compuestos es un problema fácil de resolver" es:

a) Verdad siempre.
b) Falsa siempre.
c) Depende del tamaño del número compuesto.
d) Ninguna de las anteriores.

39. ¿Cuáles de los siguientes no son modos de operación para algoritmos de cifrado por bloques?

a) CTR
b) CBC
c) CFB
d) DFB

40. Mediante un sistema criptográfico simétrico, un usuario A (con claves pública Pa y privada Ka) desea comunicarse con otro usuario B (con claves pública Pb y privada Kb). ¿De qué forma podría A enviarle un mensaje (M) a B de manera que sólo pueda verlo B y garantizando que ha sido A el que lo ha enviado?

a) Kb(Pa(M)).

b) Pb(Ka(M)).

c) Pb(M).

d) Ka(M).

41. Cuál es la longitud de la clave utilizada por el sistema criptográfico simétrico DES:

a) 56 Bits

b) 168 Bits

c) 256 Bits

d) Puede ser cualquiera, pero la habitual es 1.024 Bits

42. El estándar de sintaxis de intercambio de información personal es:

a) PKCS#7

b) PKCS#9

c) PKCS#12

d) PKCS#14

43. ¿Cuál de los siguientes cifrados simétricos es de flujo?

a) RC-4

b) IDEA

c) RC-5

d) AES

44. Señale la opción FALSA respecto a sistemas criptográficos:

a) En un sistema de cifrado de clave asimétrica, la seguridad radica en la transmisión de la clave mediante canal seguro entre el emisor y el receptor del mensaje.

b) La criptografía asimétrica incluye sistemas basados en factorización entera, el problema del logaritmo discreto y el problema del logaritmo discreto elíptico.

c) La criptografía asimétrica se fundamenta en la imposibilidad práctica de resolver ciertos problemas matemáticos de forma eficiente.

d) Dos de las aplicaciones principales de la criptografía de clave pública son el intercambio seguro de claves privadas y la firma digital.

45. Las funciones resumen (hash) MD5 y SHA-1 tienen en común:

a) Que ambas admiten mensajes de entrada de longitud máxima 264 Mbytes.

b) Que ambas generan resúmenes de 128 bits.

c) Que ambas realizan relleno de bits (si procede) en el último bloque del mensaje.

d) Que ambas realizan 80 iteraciones por bloque del mensaje.

46. Firmar un mensaje electrónico:

a) Es lo mismo que cifrarlo

b) Garantiza la confidencialidad

c) Es lo mismo que codificarlo

d) Garantiza la integridad, autenticación y no repudio

47. ¿En qué nivel del modelo OSI se realiza el cifrado?

a) 1

b) 5

c) 7

d) 6

48. En un entorno con criptografía asimétrica, para enviar un mensaje cifrado que sólo ha de ver el receptor, se ha de cifrar con:

a) La clave privada del receptor
b) La clave privada del emisor
c) La clave pública del receptor
d) La clave pública del emisor

49. Si a un mensaje le aplicamos una función hash, ciframos el resultado con una clave privada y se lo enviamos a un tercero junto con el mensaje original conseguimos:

a) Autenticación, Integridad y No repudio en origen.
b) Confidencialidad, Integridad y No repudio en origen.
c) Autenticación, Confidencialidad e Integridad.
d) Autenticación, Confidencialidad y No repudio en origen.

50. ¿Cuál de los siguientes modos de funcionamiento NO se corresponde con el algoritmo de cifrado DES?

a) Modo ECB (Electronic CodeBook).
b) Modo CBC (Cipher Block Chaining).
c) Modo OFB (Output FeedBack).
d) Modo UBC (Uncipher Block Chaining).

51. Diffie y Hellman inventaron:

a) Un algoritmo criptográfico
b) Un mecanismo de intercambio de claves
c) Las infraestructuras de clave pública (PKI))
d) Las funciones resumen

52. El test de rachas utilizado en criptografía se basa en:

a) El análisis de la independencia de los elementos de un criptograma
b) La búsqueda de las posibles dependencias o recursiones de un criptograma
c) La búsqueda de independencia entre símbolos de un criptograma
d) El análisis de la dependencia entre símbolos de un criptograma

53. PGP, o Pretty Good Privacy:

a) Fue desarrollado por Phil Zimmerman
b) Utiliza IDEA o MD5 como encriptacion
c) Utiliza TripleDES Como encriptacion
d) Ninguna de las anteriores respuestas es correcta

54. Sal (salt) en criptografía…

a) Es un algoritmo de cifrado de bloques
b) Comprende bits aleatorios que se usan como una de las entradas en una función derivadora de claves
c) Las sales hacen mucho más lentos los ataques de diccionario y los ataques de fuerza bruta
d) B y C son correctas

55. ¿Cuál de los siguientes criptosistemas se corresponde con un criptosistema asimétrico ó de clave pública?

a) IDEA (International Data Encryption Standard)
b) Algoritmo de intercambio de claves de Diffie- Hellman
c) AES (Advanced Encryption Standard)
d) RC-5

56. ¿Cuál de las siguientes afirmaciones es la correcta dentro de un sistema de cifrado asimétrico?

a) Los extremos que se comunican deben conocer la clave privada.
b) Se utiliza un par de claves, una para cifrar y otra para descifrar.
c) Utilizan longitudes de claves menores que el cifrado simétrico.
d) Es más rápido que el cifrado simétrico.

57. Señale la opción correcta sobre el hash:

a) La longitud del hash varía en función del tamaño del mensaje.
b) Para su implementación se considera más seguro emplear MD5 frente a SHA-2.
c) La función hash no es reversible, sino unidireccional.
d) Dos mensajes diferentes podrían producir la misma firma.

58. Aquel estándar de la W3C de XMLDSig cuya XMLSignature se encuentra envolviendo el documento firmado es:

a) Enveloped
b) Detached
c) Enveloping
d) Todos los documentos firmados con XMLDSig están envueltos por la XMLDSig

59. ¿Cuál es la longitud efectiva aproximada de clave del algoritmo Triple DES?

a) 112 (2x56) bits
b) 128 (2x64) bits
c) 168 (3x56) bits
d) 192 (3x64) bits

60. ¿Qué se conoce por SHA-2?

a) Una función de compresión
b) Un mecanismo de intercambio de claves
c) Una infraestructura de clave pública (PKI))
d) Un conjunto de funciones resumen

61. ¿Cuál de los siguientes algoritmos se basa en el problema de factorización entera?

a) el algoritmo RIPEMD-160
b) los algoritmos RSA y RW
c) los algoritmos DHE y DSAE
d) el algoritmo Rijndael

62. El algoritmo MD5:

a) Es un algoritmo de cifrado asimétrico.
b) Es un algoritmo de cifrado simétrico.
c) Es un algoritmo de función hash.
d) Es un algoritmo de almacenamiento de la clave privada.

63. En relación con los modos de operación fundamentales de los algoritmos hash:

a) El modo de operación MDC sirve para la verificación de integridad de mensajes
b) MAC permite comprobar tanto la integridad como la autenticidad del origen de un mensaje a través de una clave compartida
c) HMAC de IPSec es un ejemplo de implementación de MAC
d) Todas las respuestas son verdaderas

64. Las funciones "hash" en los procesos de firma electrónica se emplean para:

a) Garantizar la integridad de lo firmado.

b) Asegurar la confidencialidad de lo firmado.

c) Autenticar al firmante.

d) Asegurar el no repudio del firmante.

65. La propiedad de una función resumen por la que dado un mensaje (x), es computacionalmente imposible encontrar otro mensaje (x') cuya función resumen sea igual a la función resúmen del primer mensaje (x), corresponde a:

a) Resistencia a la preimagen

b) Resistencia a la segunda preimagen

c) Resistencia a colisión

d) Resistencia a la igualdad

66. Sobre la criptografía híbrida:

a) El transmisor cifra el mensaje con una clave simétrica o de sesión, y a su vez cifra esa clave simétrica con la clave privada del destinatario.

b) Es utilizada por Pretty Good Privacy.

c) También se conocen como "sobre digital".

d) B) y C) son correctas.

67. El algoritmo de cifrado IDEA es del tipo:

a) Asimétrico.

b) Simétrico por bloques.

c) Simétrico de flujo.

d) Simétrico de resumen (hash).

68. ¿Cuál o cuáles de los siguientes sistemas de criptografía pueden encontrarse dentro de la criptografía simétrica?

a) De bloques (block cipher), de flujos (stream cipher) y de resumen (hash function)

b) De flujos (stream cipher), de resumen (hash function) y de sigilo (stealth cipher)

c) De bloques (block cipher), de ocultamiento (conceal cipher) y de sellado de tiempo (time stamping cipher)

d) Las respuestas 'b' y 'c' son correctas

69. Dentro de los criptosistemas el Data Encryption Standard es el más conocido por su fácil implementación. Indicar cuál de las siguientes afirmaciones no le es aplicable:

a) La clave es única y debe ser conocida por receptor y emisor

b) La longitud de la clave es de 56 bits

c) El ciclo de permutación y sustitución se repite 16 veces

d) Este método de cifrado se conoce como de clave pública

70. En relación con las funciones hash o resumen, señale la respuesta CORRECTA:

a) El funcionamiento de la función hash implica la división del mensaje de entrada en secciones de longitud arbitraria de forma que se evite la necesidad de relleno.

b) La función MAC (Message Authentication Codes) no se puede utilizar para la generación de Códigos Seguros de Verificación.

c) Resistencia a la preimagen implica que dado un mensaje y su hash, es computacionalmente imposible calcular otro mensaje diferente que posea el mismo hash.

d) WHIRLPOOL produce un hash de 512 bits para un mensaje de entrada de longitud máxima 2^256-1 bits.

71. ¿Cuál de los siguientes NO es un modo de operación del algoritmo DES?

a) ECB
b) OCB
c) CBC
d) OFB

72. ¿Qué es lo que la Firma Digital no garantiza por si sola?

a) Autenticación
b) Integridad
c) Disponibilidad
d) No repudio

73. Señale la afirmación INCORRECTA con respecto a las funciones hash:

a) El algoritmo SHA-1 produce una salida resumen de 160 bits
b) Las funciones hash son usadas, principalmente, para resolver el problema de la confidencialidad de los mensajes

c) Resistencia a la preimagen significa que dada cualquier imagen y, es computacionalmente imposible encontrar un mensaje x tal que h(x)=y
d) Resistencia a colisión significa que es computacionalmente imposible encontrar dos diferentes mensajes x, x' tal que h(x)=h(x')

74. Los algoritmos de clave pública o asimétrica:

a) no han alcanzado la perfección matemática, hay ataques más eficaces que la fuerza bruta

b) presentan altas tasas de cifrado y descifrado
c) su distribución usando directorios públicos es compleja
d) no son compatibles con el concepto de certificado

75. Los sistemas de cifrado simétrico se basan en:

a) Cifrar con la clave privada y descifrar con la clave pública, para garantizar la autenticidad del emisor.

b) Cifrar con una sola clave, y no descifrar en el destino, para salvaguardar la integridad.
c) Cifrar y descifrar con la misma clave.
d) Cifrar con la clave pública y descifrar con la privada, para garantizar la confidencialidad.

76. La propiedad que permite identificar al generador de la información y así poder asegurar el origen de la información se denomina:

a) Confidencialidad
b) Autenticidad
c) Integridad
d) -

77. ¿Cuál de las siguientes no es una característica de una función Hash?

a) Obtiene un resultado unidireccional e irreversible
b) No hace falta una clave pues el texto cifrado depende exclusivamente del texto claro original

c) Se trata de una función libre de colisiones en sentido estricto
d) La seguridad de la función Hash radica en su carácter bidireccional

78. Al aplicar el algoritmo SHA-1 sobre una cadena de texto inicial obtendremos siempre un resultado:

a) De menor longitud que la cadena inicial

b) De la misma longitud que la cadena inicial

c) De mayor longitud que la cadena inicial

d) Ninguna de las anteriores

79. SAFER (Secure And Fast Encryption Routine) es un algoritmo de cifrado:

a) Simétrico de bloques.

b) Simétrico de flujo.

c) Asimétrico de factorización entera.

d) Asimétrico de logaritmo discreto.

80. Pilar quiere enviar un mensaje confidencial a Antonio, en un sistema de clave pública, por lo tanto existen las claves Pilar-privada / Pilar pública y Antonio privada / Antonio pública. Pilar genera su mensaje, ¿con qué clave de las cuatro lo cifrará?

a) Pilar-privada

b) Pilar-pública

c) Antonio-privada

d) Antonio-pública

81. Como todo criptosistema de clave pública, el protocolo del criptosistema RSA:

a) Tiene dos partes: Cifrado de Mensajes, Descifrado de Mensajes.

b) Se basa en la dificultad que supone resolver el <Problema de la Factorización Externa>.

c) Tiene tres partes: Generación de claves, Cifrado de mensajes, Descifrado de mensajes.

d) Se basa en la dificultad que supone resolver el <Problema de Socrates- Arquimedes>.

82. Indicar cuál de los siguientes es un algoritmo de criptografía asimétrica:

a) RSA.

b) DES.

c) Blowfish.

d) AES (Rijndael).

83. Señale aquel que se corresponde con un protocolo de establecimiento de claves entre partes:

a) Diffie Hellman

b) RIPEMD

c) Rabbit

d) Blowfish

84. La criptografía asimétrica es un método criptográfico para el envío de mensajes que usa:

a) Un par de claves privadas correspondientes a las entidades que se comunican y que solamente conocen ellos, el remitente y destinatario y que usan ambos para lograr descifrar los mensajes que se intercambian.

b) Una clave que se intercambian alternativamente entre los interlocutores para salvaguardar la información que se intercambian. Esta clave cambia nuevamente con cada nueva sesión y tiene una longitud de caracteres suficiente para evitar el apropiamiento indebido.

c) Una clave tanto para cifrar como para descifrar mensajes. Las dos partes que se comunican entre sí han de ponerse de acuerdo de antemano sobre la clave a usar. El remitente cifra un mensaje usando la clave y el destinatario lo descifra con esta misma clave.

d) Un par de claves relacionadas entre sí y que pertenecen a la misma persona: una clave pública que se puede entregar a cualquiera o publicarla en algún sitio y una clave privada que el propietario debe guardar de modo que nadie tenga acceso a ella.

85. Señale la opción correcta sobre la criptografía simétrica de bloque:

a) El uso del algoritmo DES resulta más seguro que el de AES

b) SNOW 3G es un algoritmo de este tipo de criptografía utilizado en UMTS/LTE

c) 64 Kbits y 128 Kbits son longitudes típicas de los bloques empleadas en sus algoritmos

d) Son algoritmos de este tipo de criptografía Camellia y AES/Rijndael

86. El ataque criptográfico llamado "birthday attack" está basado en la paradoja del cumpleaños. ¿Cuál es su objetivo?

a) Capturar pares de claves de funciones resumen (hash) con el mismo resultado, ya que es estadísticamente más probable el ataque probando de dos en dos.

b) Robar la clave privada del dni electrónico del usuario cuando está realizando alguna gestión con el mismo, ya que se extrae dicha clave conociendo parte de la información contenida, como la fecha de nacimiento del sujeto.

c) Averiguar la clave de acceso al facebook de un usuario sabiendo cuándo cumple años ya que la gente es muy descuidada y usa esa información como pregunta secreta.

d) Encontrar una clave en toda las aplicaciones que usa generalmente un usuario (correo, facebook, twitter, etc.) que coincida con su fecha de cumpleaños y a partir de ahí hacerse con el resto de contraseñas.

87. Entre los algoritmos que puede utilizar SSL se encuentran:

a) TripleDES, RC4 y SHA-1

b) DES, RC2 y MD5

c) Además de los anteriores puede usar SKIPJACK y RSA

d) Puede usar todos los anteriores e incluso no usar algoritmo de encriptación, pero sí de autenticación con SHA-1 o MD5

88. El algoritmo Rijndael:

a) Tiene un tamaño de clave fijo de 128 bits.

b) Tiene un tamaño de bloque fijo de 256 bits.

c) Tiene un tamaño de clave de 128, 192 o 256 bits.

d) Tiene un tamaño de clave múltiplo de 32 bits.

89. La norma técnica elaborada por la IETF (Internet Engineering Task Force) para permitir a los administradores de dominio especificar las claves utilizadas para establecer una conexión criptográficamente segura a un servidor se denomina:

a) IPSEC (Internet Protocol Security).

b) TLS (Transport Layer Security).

c) DNSSEC (Domain Name System Security Extensions).

d) DANE (DNS-based Authentication of Named Entities).

90. El servicio de seguridad que garantiza que la información no ha sido mutilada o alterada de manera no autorizada se denomina:

a) Autentificación

b) Confidencialidad

c) Integridad

d) No repudio

91. La técnica de ocultar un mensaje secreto dentro de un mensaje ordinario y extraerlo en destino se llama:

a) Algoritmo de clave secreta

b) Bytecode

c) Esteganografía

d) Dpyware

92. En el proceso de cifrado basado en el método DES de criptosistema simétrico, en el cuál existen n nodos de intercambio de mensajes, ¿cuántas claves debe gestionar cada uno de los nodos para comunicarse con el resto?

a) n

b) n + 1

c) n!

d) Ninguna de las anteriores contestaciones es cierta

93. ¿Cuál de las siguientes afirmaciones es la correcta dentro de un sistema de cifrado simétrico?

a) Se utiliza un par de claves, una para cifrar y otra para descifrar.

b) Los extremos que se comunican deben conocer la clave privada.

c) Utilizan longitudes de claves mayores que el cifrado asimétrico.

d) Es más lento que el cifrado asimétrico.

94. Indique la afirmación cierta:

a) El resultado de cifrar de nuevo un texto cifrado con otro algoritmo aporta una seguridad adicional, eso sí, implicando una carga extra de trabajo tanto para cifrar como para luego descifrar el texto

b) Los cifradores de flujo no aportan información alguna al criptoanalista que observa el texto cifrado

c) La calidad del algoritmo HASH es independiente de la calidad de la dispersión obtenida en dicho algoritmo

d) El ataque del cumpleaños no es aplicable a las funciones HASH, ya que no son reversibles

95. ¿Qué es la esteganografía?

a) Es equivalente al cifrado, especialmente en imágenes digitales, audio, ficheros y video digital.

b) Es un tipo de troyano.

c) Actualmente no se utiliza para el envío de información.

d) Es el envío de un mensaje oculto, especialmente en imágenes digitales, audio, ficheros y video digital.

96. ASCII es el acrónimo de:

a) American Standard Code for Information Integration

b) Alliance Standard Code Interchange Integration

c) American Standard Code for Information Interchange

d) All sugar can injure igloos

97. El cifrado híbrido consiste en:

a) utilizar el cifrado simétrico para intercambiar la clave pública y usar después el cifrado asimétrico.

b) utilizar el cifrado asimétrico para intercambiar la clave y usar después el cifrado simétrico.

c) alternar entre el cifrado simétrico y asimétrico para aumentar la seguridad.

d) utilizar el cifrado simétrico para intercambiar la clave secreta y usar después el cifrado asimétrico.

98. La criptografía cuántica es una técnica basada en:

a) Polarización de la luz

b) Propiedades de los campos magnéticos

c) Ultrasonidos

d) Transmisión de datos a muy alta frecuencia

99. ¿Qué es el efecto avalancha en una función hash?

a) Una pequeña variación en la longitud del mensaje debe producir una gran variación en la longitud del resumen

b) Una pequeña variación del contenido del mensaje debe producir una gran variación en la longitud del resumen

c) Una pequeña variación en el contenido del mensaje debe producir una pequeña variación en la longitud del resumen

d) Una pequeña variación en el contenido del mensaje debe producir una gran variación en el contenido del resumen

100. En relación con la criptografía simétrica, señale la opción CORRECTA:

a) AES (Rijndael) es un sistema muy robusto y utilizado a gran escala, no obstante, exige gran cantidad de memoria para el cifrado.

b) En general, existe una clave para cifrar y ora clave para descifrar, que son conocidas por emisor y receptor.

c) La criptografía simétrica de bloque se suele utilizar en aplicaciones en tiempo real con claves de 128 bits.

d) AES es más seguro y más rápido que 3DES.

101. La seguridad de los algoritmos de cifrado debe basarse en:

a) Mantener el funcionamiento de los algoritmos en secreto.
b) Utilizar sistemas propietarios.
c) Demostrar su resistencia desde un punto de vista teórico y práctico.
d) Utilizar tarjeta electrónica.

102. Cuál de los siguientes NO es un algoritmo de funciones hash:

a) SHA-256.
b) BASH.
c) WHIRLPOOL.
d) HAVAL.

103. Señale la falsa:

a) CRL son las siglas en inglés de la lista de certificados revocados
b) OCSP son las siglas en inglés del protocolo de estado de certificados en línea
c) PKCS#7 corresponde al estándar del formato del sobre digital
d) PKCS#11 corresponde al algoritmo RSA

104. SHA-1 produce un valor hash de:

a) 20 bytes.
b) 33 bytes.
c) 256 y 512 bits, respectivamente.
d) 256 bits.

105. Indique cuál de las siguientes funciones relativas a una PKI es INCORRECTA:

a) Garantiza mediante el uso de certificados digitales el no repudio, integridad, autenticación y la publicación de los datos transmitidos.

b) Los componentes de una PKI para la administración de los certificados son: software, hardware, personas, políticas, procedimientos.

c) Entre las funciones de una PKI se encuentra la revocación de claves.

d) Entre las funciones de una PKI se encuentran la generación, recuperación y renovación de claves.

106. ¿Cuál de los siguientes algoritmos es más eficienté para cifrar grandes volúmenes de datos?

a) SHA-2

b) RSA

c) AES

d) MDM-5

107. ¿Cuál de las siguientes NO es cierta con relación a una función hash o resumen?

a) La función hash es unidireccional

b) La longitud del hash varía con el tamaño del mensaje

c) WHIRLPOOL es un algoritmo basado en función hash

d) -

108. Señale la respuesta INCORRECTA respecto a las funciones criptográficas hash o resumen:

a) MD5 genera un hash de 128 bits.

b) SHA-1 genera un hash de 160 bits.

c) Se conoce por SHA-2 a un conjunto de funciones de la familia SHA que generan hashes de longitud 224, 256, 384 y 512 bits.

d) La longitud mínima del hash soportada en SHA-3 es 256 bits.

109. ¿Cuál de las siguientes algoritmos no es de clave simétrica?

a) AES

b) DSA

c) DES

d) BlowFish

110. Los criptosistemas pueden clasificarse en:

a) Concretos, Estables e Inestables.

b) Simétricos, Paralelos y Referenciales.

c) Asimétricos, Referenciales y Concretos.

d) Simétricos, Asimétricos e Híbridos.

111. El Teorema Chino del Resto es un método matemático de resolución de ecuaciones en aritmética modular que tiene aplicación principalmente en:

a) Criptografía asimétrica o de clave pública

b) Criptografía simétrica

c) Cálculo de impedancias de cables coaxiales

d) Junto con el teorema de Euler se usa en resolución de caminos en grafos, teniendo su aplicación práctica en la resolución de enrutamientos en comunicaciones

112. Un sistema compuesto por 15 usuarios intercambian información cifrada mediante AES. Si los canales de comunicación entre usuarios es 2 a 2 (es decir, todos intercambian información con todos) ¿cuántas claves son necesarias?

a) 15

b) 105

c) 210

d) 30

113. ¿Cuál es la longitud equivalente a una clave RSA de 1024 bits si utilizáramos un algoritmo de clave simétrica?

a) 132 bits.

b) 80 bits.

c) 64 bits.

d) 512 bits.

114. En una comunicación HTTPS, ¿qué tipo de cifrado se utiliza?

a) Tanto el simétrico como el asimétrico.

b) Asimétrico exclusivamente.

c) Simétrico exclusivamente.

d) -

115. Señale la correcta:

a) 3DES es un algoritmo de cifrado asimétrico que consiste en aplicar tres veces DES

b) AES es un algoritmo muy versátil porque puede usarse como algoritmo de bloque, como algoritmo de flujo, como función resumen y como generador de números pseudo-aleatorios

c) Las características de las funciones hash son: resistencia a la preimagen, resistencia a la postimagen y resistencia a la colisión

d) Todas las anteriores

116. Indique la afirmación INCORRECTA sobre el algoritmo DES (Data Encryption Standard):

a) Está basado en las redes de Feistel

b) Usa una clave de 56 bits

c) Roto en 1997 mediante búsqueda exhaustiva

d) Para hacerlo más robusto se utiliza el doble DES 2-DES

117. ¿Cuál de los siguientes algoritmos criptográficos es de tipo asimétrico?

a) Triple DES (TDES)

b) Rinjdael (AES)

c) Diffie-Hellman

d) IDEA (International Data Encription Algorithm)

118. El sistema de encriptación RSA (Rivest, Shamir y Adleman, 1978)…:

a) El receptor del mensaje debe conocer la clave pública para descifrarlo

b) Se basa en la seguridad que confiere la dificultad de factorizar números grandes

c) Es un sistema de encriptación simétrico

d) Garantiza la seguridad aún utilizando números primos de menos de veinte cifras

119. Marcar la correcta respecto de los algoritmos criptográficos:

a) El algoritmo de cifra de Merkle-Hellman es de clave dispersa

b) El algoritmo de cifra de Merkle-Hellman es de clave única

c) El algoritmo DES es de clave pública

d) El algoritmo DES es de clave simétrica

120. En los criptosistemas asimétricos:

a) El emisor cifra con la clave pública del receptor y el receptor descifra con la clave pública del emisor

b) El emisor cifra con su clave pública y el receptor descifra con su clave privada

c) El emisor cifra con la clave pública del receptor y el receptor descifra con su clave privada

d) El emisor cifra con su clave privada y el receptor descifra con su clave pública

121. En una operación de resumen o hash, con h = H(M):

a) M debe ser de longitud fija

b) no tiene por qué conocerse H

c) h debe ser de longitud fija

d) dado M, no siempre se va a poder calcular H(M)

122. Señale la opción INCORRECTA sobre las funciones hash o resumen:

a) Su utilización en MDC (Modification Detection Codes) permite verificar la integridad de los mensajes.

b) La longitud del hash es siempre la misma, con independencia del tamaño del mensaje.

c) La función hash es reversible y bidireccional.

d) Entre los algoritmos utilizados se encuentran MD5 y SHA-2.

123. En una tabla hash, si la función hash utilizada da el mismo índice para dos valores que se están insertando:

a) La premisa es falsa; por definición, una función hash nunca puede dar el mismo resultado para dos valores distintos.

b) El segundo elemento tendría que sobreescribir al primero.

c) El segundo elemento podría almacenarse en alguna otra posición libre de la tabla hash.

d) En una tabla hash no se puede utilizar una función hash que pueda dar el mismo resultado para dos valores distintos.

124. Se define como criptosistema asimétrico lo siguiente:

a) algoritmo basado en clave única

b) algoritmo basado en 2 claves, una de cifrado y otra de descifrado, siendo una pública y otra privada

c) algoritmo basado en 2 claves, una de cifrado y otra de descifrado, siendo ambas privadas

d) Ninguna de las anteriores

125. Señale la afirmación CORRECTA:

a) DES es un algoritmo de cifrado asimétrico

b) RSA es un algoritmo de cifrado simétrico

c) AES es implementable tanto en hardware como en software

d) Todas las anteriores son FALSAS

126. Seleccione la opción correcta, de entre las siguientes, si se desea enviar un mensaje cifrado a otra persona utilizando claves asimétricas para evitar que sea leído por terceros:

a) Se encriptará con la clave privada del emisor para que el receptor lo descifre utilizando la clave pública del emisor.

b) Se encriptará con la clave privada del receptor para que el receptor lo pueda descifrar utilizando su clave pública.

c) Se encriptará con la clave pública del emisor para que el receptor lo descifre utilizando la clave privada del emisor.

d) Se encriptará con la clave pública del receptor para que el receptor lo pueda descifrar utilizando su clave privada.

127. En relación con la criptografía asimétrica, señale la respuesta CORRECTA:

a) Las claves pueden ser más cortas en criptografía elíptica para una fortaleza similar a otros algoritmos asimétricos con mayor longitud de clave, por lo que se utilizan claves de 64 o 128 bits.

b) La vulnerabilidad del algoritmo RSA no depende del generador aleatorio de números primos.

c) La criptografía asimétrica de 1.024 bits se considera equivalente a la simétrica de 112 bits.

d) Para las aplicaciones más críticas, como la raíz de una infraestructura de clave pública (PKI), se suelen utilizan claves RSA de 4.096 bits.

128. La especificación PKCS#3 de RSA se refiere a:

a) El estándar criptográfico RSA.

b) La sintaxis de la información de clave privada.

c) El intercambio de claves Diffie-Hellman.

d) La sintaxis del mensaje criptográfico.

129. SSL/TLS:

a) Permite a un comercio en internet cobrar a sus clientes, efectuando la transacción por medio de un tercero de confianza (banco)

b) Permite que un tercero con acceso al tráfico entre el servidor y el cliente no pueda romper la confidencialidad

c) Es un algoritmo de cifrado, de un número de bits variable

d) Ninguna de las anteriores respuestas es correcta

130. Los cifradores de clave secreta:

a) Pueden encadenarse (cifrado producto) produciendo un criptograma más robusto que el obtenido al aplicar un único cifrado.

b) A igualdad de longitud de clave son más robustos que los de clave pública.

c) Su seguridad recae en el secreto del diseño.

d) Se usan en los sistemas operativos Windows XP y 7 para proteger las contraseñas de los usuarios.