Test Tema 79 #2

Actualizado el 13/04/2025

1. De los siguientes algoritmos criptográficos señale cuál es de clave pública:

a) DES (Data Encryption Standard)
b) RSA (Rivest, Shamir, Adelman)
c) IDEA (International Data Encryption Algorithm)
d) LOKI

2. 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

3. Las técnicas orientadas a garantizar la seguridad en las operaciones relacionadas con los servicios de certificación y firma electrónica, deben cumplir los principios de:

a) Confidencialidad, Seguridad, Integridad, y Autenticación.
b) Confidencialidad, Integridad, Autenticación, y No Repudio.
c) Disponibilidad, Integridad, Autenticación, y No Repudio.
d) Disponibilidad, Seguridad, Integridad, y Autenticación.

4. ¿Cuál es la equivalencia en criptografía asimétrica a una longitud de clave de 112 bits en criptografía simétrica?

a) 1102 bits.
b) 1768 bits.
c) 2048 bits.
d) 3072 bits.

5. ¿Por qué el algoritmo DSA no sirve para cifrar?

a) Porque al realizar funciones modulo x (donde x es uno de los valores públicos del sistema) no se puede realizar su inversión

b) Porque realiza un hash del mensaje, por tanto no es recuperable
c) Porque tendríamos que enviar la clave privada
d) No es cierto, el algoritmo DSA sí sirve para cifrar

6. El algoritmo SHA-1 (RFC 3174) produce un resumen de salida de:

a) 128 bits
b) 160 bits
c) 224 bits
d) 256 bits

7. Dentro de los sistemas de criptografía de resumen podemos encontrar los algoritmos:

a) DES
b) SEAL
c) RC-4
d) MD-5

8. Sean en una comunicación: m = mensaje a transmitir. y = h(m) el código hash del mensaje m calculado en origen. m' = mensaje recibido. y' = h(m') el código hash del mensaje m' recibido, calculado en destino. Señalar cuál de las siguientes afirmaciones es cierta:

a) Si y = y' entonces se puede afirmar que la integridad de m está garantizada en m'.

b) Si y = y' entonces se puede afirmar que la clave privada ha sido alterada.

c) Si m = m' entonces se puede afirmar que la confidencialidad de y está garantizada en y'.

d) Si y = y' entonces se puede afirmar que la confidencialidad de m está garantizada en m'.

9. La distancia de Hamming entre las palabras 01000 y 01010 es:

a) 1

b) 2

c) 3

d) 4

10. Respecto al algoritmo de cifrado RC5, señale la respuesta correcta:

a) Se trata de un algoritmo de cifrado asimétrico.

b) No utiliza rotaciones dependientes de los datos para su proceso.

c) Posee un número fijo de rotaciones para su proceso.

d) Posee tamaño variable de clave.

11. De entre los siguientes estándares XML del W3C, ¿Cuál define políticas de control de acceso de usuarios?

a) DSML

b) XrML

c) XKMS

d) XACML

12. ¿Qué algoritmo de cifrado fue designado por la Administración Federal Americana como estándar de cifrado sucesor del algoritmo DES?

a) Triple DES

b) AES

c) IDEA

d) Blowfish

13. ¿Cuál de estos estándares o métodos pertenece a la criptografía de clave pública?

a) Triple DES (Estándaride Encriptación de Datos)

b) AES (Estándar de Entriptación Avanzada)

c) El método RSA (iniciales de Rivest, Shamir y Adleman)

d) HES (Estándar de Encriptación Holística)

14. Indique cuál de los siguientes NO es, actualmente, un tamaño de clave válido para el algoritmo de cifrado AES:

a) 128 bits

b) 192 bits

c) 256 bits

d) 512 bits

15. En relación con la huella digital y las funciones hash, señalar la opción falsa:

a) Dos mensajes idénticos, producen la misma huella

b) Dada una huella es computacionalmente imposible encontrar un mensaje que produzca esa huella

c) Si dos huellas son idénticas, sólo pueden haber sido originadas con el mismo mensaje

d) Si dos huellas son idénticas, pueden haber sido originadas por distintos mensajes con muy poca probabilidad

16. RSA es:

a) Un algoritmo criptográfico

b) Un mecanismo de intercambio de claves

c) Una infraestructura de clave pública (PKI))

d) Una función resumen

17. ¿Cuál de las siguientes afirmaciones es falsa respecto al uso de mecanismos criptográficos?

a) El uso de mecanismos criptográficos puede aumentar la latencia de las comunicaciones

b) El uso de mecanismos criptográficos puede aumentar la confidencialidad

c) El uso de mecanismos criptográficos puede implementarse por software o por hardware

d) El uso de mecanismos criptográficos no puede proporcionar integridad en las comunicaciones

18. ¿Cuál de las siguientes no es una propiedad que debe cumplir una función resumen (hash)?

a) Resistencia a la preimagen

b) Resistencia a la colisión Fuerte

c) Resistencia a la colisión Suave

d) Resistencia a la no colisión

19. Indique cuál de los siguientes algoritmos criptográficos NO ha sido autorizado para uso en el Esquema Nacional de Seguridad según la guía CCN-STIC 807:

a) MD5

b) TDEA

c) AES

d) RSA

20. Las aplicaciones fundamentales de la criptografía asimétrica son:

a) El cifrado eficiente y la firma digital

b) El intercambio seguro de claves privadas o de sesión y la firma digital

c) El intercambio seguro de claves privadas o de sesión y el cifrado eficiente

d) Todas las anteriores

21. ¿Qué longitudes de clave tienen las diferentes versiones del algoritmo AES reconocidas oficialmente por el NIST?

a) 64, 128, 256 bits

b) 128, 192, 256 bits

c) 128, 256, 512 bits

d) 128, 256, 384 bits

22. Uno de los objetivos de la seguridad es evitar que alteren los datos durante una transmisión, esto es conocido como:

a) Integridad

b) Confidencialidad

c) No Repudio

d) Disponibilidad

23. El grupo de estándares de criptografía de clave pública, PKCS (Public Key Cryptography Standars), son publicados por:

a) IEEE
b) IETF
c) RSA
d) DES

24. En criptografía asimétrica, con que clave cifra un usuario un documento:

a) Con su propia clave privada
b) Con su propia clave pública
c) Con la clave privada del destinatario
d) Con la clave pública del destinatario

25. ¿Cuál es la longitud del resumen de la función SHA-1?

a) 64 bits
b) 128 bits
c) 160 bits
d) 224 bits

26. Señale cuál de los siguientes algoritmos es de cifrado asimétrico:

a) Cast5
b) Twofish
c) Idea
d) ElGamal

27. Ordene de forma decreciente, en relación al coste en hardware (puertas lógicas equivalentes), las siguientes primitivas criptográficas: función resumen (ej. MD5 o SHA-1), cifrado asimétrico (ej. RSA o curvas elípticas) y cifrado simétrico (ej. AES o DES):

a) Función resumen, Cifrado asimétrico, Cifrado simétrico.
b) Función resumen, Cifrado simétrico, Cifrado asimétrico.
c) Cifrado asimétrico, Cifrado simétrico, Función resumen.
d) Cifrado asimétrico, Función resumen, Cifrado simétrico.

28. En el protocolo de envoltura digital, o sistema de cifrado mixto, como sucede cuando se establece una sesión TLS, el emisor y el receptor usan:

a) Cifrado simétrico para intercambiar la clave de sesión.
b) Cifrado asimétrico para intercambiar la clave de sesión.
c) Un canal externo para intercambiar la clave de sesión.
d) La clave de sesión para autenticarse.

29. Respecto al algoritmo DSA, ¿cuál de estas afirmaciones es falsa?

a) Sirve para firmar documentos
b) Sirve para autenticar
c) Sirve para cifrar
d) Es un estándar de FIPS para firmas digitales

30. ¿Qué algoritmo utiliza el cifrado por bloques?

a) ElGamal
b) DSA
c) RSA
d) DES

31. ¿Cuál de las siguientes afirmaciones referentes a un sistema criptográfico de clave pública o asimétrico es falsa?

a) Cada usuario posee dos claves denominadas pública y privada, independientes entre sí. La clave privada es la usada en el servicio de confidencialidad (cifrado)

b) La criptografía de clave pública se usa para la implantación de servicios de seguridad avanzados como: autenticidad (firma digital), no repudio, prueba de entrega e integridad, entre otros

c) El uso de criptografía de clave pública, por ejemplo RSA, para servicios de confidencialidad (cifrado) proporciona un rendimiento muy inferior (caracteres cifrados/segundo) al proporcionado por los algoritmos simétricos como el DES

d) La gestión de claves de los sistemas criptográficos asimétricos es sencilla, comparada con la existente en los sistemas convencionales simétricos de clave secreta

32. Como algoritmos de cifrado simétrico de bloque no figura:

a) Lucifer

b) Serpent

c) Seal

d) Shark

33. Los documentos de la serie PKCS son especificaciones producidas por los Laboratorios RSA. Señale la falsa:

a) PKCS#3 Protocolo de acuerdo de claves Diffie-Hellman

b) PKCS#11 Cryptoki

c) PKCS#1 Standard de encriptación RSA

d) Todas son ciertas

34. Señale la afirmación errónea respecto a los algoritmos de cifrado:

a) Si utilizamos el sistema de cifrado mediante clave pública en una red local de N nodos, para poder comunicarse con todos los demás, cada nodo deberá conocer N - 1 claves, y serán necesarias un total de N! / 2 x (N - 2)! parejas de claves

b) Si utilizamos el sistema de cifrado mediante clave simétrica en una red local de N nodos, para poder comunicarse con todos los demás, cada nodo deberá conocer N - 1 claves, y serán necesarias un total de N*(N-1)/2 claves

c) Si utilizamos el sistema de cifrado mediante clave simétrica en una red local de 10 nodos, para poder comunicarse con todos los demás, cada nodo deberá conocer 9 claves, y serán necesarias un total de 45 claves

d) Los algoritmos de cifrado mediante clave simétrica DES, RC-2 y RC-4 son públicos. A partir de un bloque de caracteres “en claro”, estos algoritmos generan un bloque de caracteres ininteligible (cifrado) mediante un número de sustituciones y permutaciones

35. De las siguientes opciones, la capa que proporciona cifrado al protocolo HTTPS (Hypertext Transfer Protocol Secure) es:

a) S-HTTP (Secure-HTTP)

b) IPSec (Internet Protocol Security)

c) IKE (Internet Key Exchange)

d) TLS (Transport Layer Security)

36. El algoritmo de cifrado Rijndael puede ser especificado por una clave:

a) Fija de 256 bits

b) Con un mínimo de 128 bits y un máximo de 256 bits

c) Fija de 128 bits

d) Con un mínimo de 256 bits y un máximo de 1024 bits

37. SHA-1 es un algoritmo empleado por la criptografía simétrica de:

a) Resúmen

b) Bloques

c) Flujos

d) Las respuestas ‘b’ y ‘c’ son correctas

38. ¿Cuál de las siguientes afirmaciones no es verdadera respecto a la criptografía?

a) Los algoritmos "stream" son los más rápidos
b) Los algoritmos "stream" y "block" son equiparables
c) La velocidad no tiene ninguna correlación con la longitud de clave
d) 3DES es más seguro y lento que DES

39. ¿Cuáles de los siguientes sistemas de criptografía pueden encontrarse dentro de la criptografía simétrica?

a) De métodos y de funciones.
b) De bloque y de flujo.
c) De ocultamiento y de resumen.
d) De funciones y de flujo.

40. Con el cifrado se asegura:

a) la autenticidad
b) la confidencialidad
c) la integridad, la autenticidad y el no repudio en destino
d) la integridad, la autenticidad y el no repudio en origen

41. La rotura de la máquina de cifrado Enigma es un ejemplo de:

a) Criptografía asimétrica o de clave pública
b) Cifrado César
c) Criptoanálisis
d) Criptografía cuántica

42. Al ataque criptográfico consistente en el barrido del espacio de claves se le denomina:

a) Fuerza bruta
b) Criptoanálisis diferencial
c) Criptoanálisis lineal
d) Análisis de temporización

43. ¿Cuál de las siguientes opciones es una función hash actualmente segura?

a) MD5
b) RSA
c) SHA-3
d) 3DES

44. En criptografía simétrica, ¿qué es una sustitución monoalfabética monográmica?

a) Cada letra del mensaje original es sustituido por sólo una otra letra, número o símbolo
b) Buscan paliar la sensibilidad frente a ataques basados en el estudio de frecuencias de símbolos
c) Cada letra del mensaje original puede ser sustituida por más de una letra, número o símbolo
d) La que sustituye las letras en grupos de longitud variable, dependiendo de su posición dentro del mensaje

45. ¿En qué protocolo se basa el intercambio automático de claves utilizado en IKE?

a) GRE
b) HMAC
c) DH
d) RSA

46. ¿Cuál NO es una característica de la Huella Digital?

a) Dos mensajes iguales producen la misma huella digital

b) Conocido un mensaje M1 y su resumen R, será computacionalmente imposible encontrar otro mensaje M2 cuyo resumen sea también R

c) Dos mensajes parecidos producen huellas digitales diferentes

d) La función hash es reversible

47. En un sistema con 10 usuarios se plantea el uso de un sistema criptográfico para asegurar las transferencias de datos entre todos ellos. ¿Cuál sería la diferencia entre usar sistemas de claves simétricas o asimétricas?

a) No existe diferencia, en ambos casos se necesitarán 20 claves.

b) Con el sistema asimétrico hacen falta 20 claves y con el simétrico el doble, ya que todas son secretas.

c) Con el sistema asimétrico hacen falta 20 claves y con el simétrico sólo 10, una por cada usuario.

d) Con el sistema asimétrico hacen falta 20 claves y con el simétrico 45 claves.

48. ¿Cual de los siguientes algoritmos de cifrado, es de clave asimétrica?

a) AES

b) 3DES

c) RSA

d) RC5

49. La autenticación consiste en:

a) Comprobar los permisos del usuario

b) Comprobar que los datos no han sido alterados en una comunicación

c) Garantizar que ninguna de las partes pueda negar una operación realizada

d) Comprobar la identidad del usuario

50. De entre los siguientes, indique cuál no es un sistema criptográfico de clave simétrica:

a) DES

b) Triple DES

c) RSA

d) IDEA

51. El protocolo SSL v3:

a) Trabaja tanto sobre TCP como sobre UDP

b) Hasta hace pocos años los navegadores que incorporaban TLS/SSL tenían su exportación desde EEUU limitada a claves de 128 bits

c) Es idéntico al protocolo TLS, aunque este último está normalizado por el IETF mediante un RFC

d) Intercambia las claves secretas mediante el ensobrado digital (digital envelopment) o mediante Diffie-Hellman

52. La criptografía sirve para codificar:

a) Lenguaje manuscrito

b) Lenguaje manuscrito y datos

c) Datos exclusivamente, al no poder aplicar técnicas informáticas al lenguaje manuscrito

d) La criptografía no se usa para codificar, sino sólo para decodificar

53. Un sistema criptográfico que utiliza pares de claves (pública y privada) para cifrar y descifrar información se denomina:

a) Simétrico.
b) Asimétrico.
c) Paralelo.
d) Redundante.

54. En los sistemas criptográficos híbridos:

a) Se prescinde del cifrado simétrico
b) Se cifra la clave de sesión mediante un cifrado simétrico
c) Se cifra la clave de sesión mediante un cifrado asimétrico
d) Se omite el uso de certificados digitales, cuando se dispone de plataformas PKI

55. ¿Qué es HSM?

a) Un dispositivo criptográfico basado en hardware que genera, almacena y protege claves criptográficas

b) Un algoritmo de clave pública
c) Un API genérico de acceso a dispositivos criptográficos
d) Un conjunto de políticas de seguridad en el ámbito de la criptografía de clave púbica

56. ¿Cuál de los siguientes algoritmos no es de criptografía simétrica de flujos?

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

57. ¿Cuál de las siguientes afirmaciones sobre procedimientos de cifrado en flujo es CIERTA?:

a) Forman parte de los criptosistemas de clave pública.
b) Forman parte de los criptosistemas de cifrado en bloque.
c) Forman parte de los criptosistemas de clave secreta.
d) Ninguna de las afirmaciones anteriores.

58. Técnica de cifrado utilizada por los clientes de correo-electrónico:

a) MD5
b) IDEA
c) Curva Elíptica
d) S/MIME

59. En lo que concierne a los algoritmos de cifrado, la recomendación PKCS#7 de la compañía RSA, se refiere a:

a) Formato del sobre digital.
b) Formato del certificado digital.
c) Sintaxis de la clave privada.
d) Algoritmo Diffie-Hellman.

60. En el ámbito de la criptografía asimétrica, ¿cuál de las siguientes afirmaciones es cierta?

a) La clave pública sirve para firmar los documentos, antes de enviarlos.
b) La clave privada sirve para cifrar la clave pública antes de firmar con esta última un documento.

c) La clave privada se ha de generar aleatoriamente a partir de la clave pública cada vez que se firma un documento.

d) La clave pública sirve para comprobar la firma digital de un documento firmado.

61. La clave pública forma parte de un:

a) Sistema criptográfico simétrico
b) Sistema criptográfico analógico
c) Sistema criptográfico asimétrico
d) Sistema criptográfico propietario de la Administración Pública

62. A la hora de atacar un texto cifrado, el método que explota las debilidades del algoritmo de cifrado o sus puntos menos fuertes para intentar deducir un texto nativo o deducir la clave de cifrado se denomina:

a) Ataque por Fuerza Bruta
b) CriptoAnálisis
c) Análisis Diferencia de Cifrado
d) CriptoCifrado

63. Los algoritmos de clave simétrica:

a) Disponen de un par de claves pública/privada
b) Son menos eficientes que los de clave asimétrica
c) Se pueden distribuir y mantener fácilmente las claves
d) Tienen una alta velocidad de cifrado y descifrado

64. CRAM-MD5 definido en el RFC 2195 es una técnica criptográfica que consiste en:

a) Un mecanismo de autenticación challenge-response para autenticación de usuarios POP e IMAP, entre otros.

b) Un mecanismo de cifrado simétrico de bloque basado en una clave compartida y derivación de subclaves usando MD5.

c) Un algoritmo de firma electrónica basado en MD5, ideado para escenarios en los que no puede usarse criptografía asimétrica.

d) Un algoritmo de cifrado simétrico de flujo (stream) basado una clave compartida, en MD5 y un LFSR predeterminado.

65. ¿Cuál es el tamaño de bloque del algoritmo DES?

a) 64 bits
b) 56 bits
c) 128 bits
d) 256 bits

66. En criptografía simétrica, ¿qué es una sustitución monoalfabética?

a) Emplean un alfabeto de salida con más símbolos que el alfabeto de entrada
b) Buscan paliar la sensibilidad frente a ataques basados en el estudio de frecuencias de símbolos

c) Se sustituye cada carácter del texto original siempre por otro carácter determinado
d) La que sustituye las letras en grupos de longitud variable, dependiendo de su posición dentro del mensaje

67. RSA es:

a) Un algoritmo de clave privada
b) Un algoritmo de clave pública
c) Un método de criptoanálisis diferencial
d) Una infraestructura de clave pública

68. Atendiendo únicamente a criterios de eficiencia en tiempo, ¿cuál de los siguientes métodos sería el más eficiente para securizar las comunicaciones entre usuarios dentro de una red?

a) Mediante claves simétricas.
b) Mediante claves asimétricas.
c) Mediante claves simétricas compartidas periódicamente con claves asimétricas.
d) Mediante claves asimétricas compartidas periódicamente con claves simétricas.

69. Indique cuál de las siguientes afirmaciones es cierta:

a) Las funciones hash se utilizan en los mecanismos de cifrado/descifrado de mensajes.
b) Las funciones hash se pueden utilizar para garantizar la integridad de los mensajes transmitidos.
c) Las funciones hash generan valores cuya longitud, en bits, depende de la longitud del mensaje original.
d) Las funciones hash requieren el uso de claves de cifrado.

70. El algoritmo de encriptación Camellia:

a) Fue desarrollado en EEUU.
b) La longitud de clave es variable entre 128, 192 y 256 bits.
c) Tiene un tamaño de bloque de 64 bits.
d) No está soportado en TLS/SSL.

71. ¿Qué algoritmo genera un Hash de mayor longitud?

a) MD5
b) SHA-1
c) SHA-384
d) WHIRLPOOL

72. Los criptosistemas irreversibles:

a) No existen actualmente dada la potencia de los sistemas actuales y la potencia de la computación distribuida
b) Se utilizan sobre todo para la autenticación de entidades
c) Se basan en funciones matemáticas no invertibles computacionalmente, o carentes de inversa
d) B y C son ciertas

73. Cuál de los siguientes NO es una forma básica de funcionamiento o modo de operación con los bloques de mensajes en los algoritmos simétricos de cifrado:

a) Cipher Block Chainning (CBC).
b) Cipher FeedBack (CFB).
c) Output FeedBack (OFB).
d) Quadruple Block Cipher (QBC).

74. El cifrado TDES - 2EDE (Encrypt-Decrypt-Encrypt) es:

a) Un cifrado doble con 2 claves que aumentan el tamaño de la clave DES a 112 bits
b) Un cifrado triple con 2 claves que aumenta el tamaño de la clave DES a 112 bits
c) Un cifrado triple con una clave de 56 bits
d) No existe

75. En el protocolo Secure Socket Layer (SSL) el subprotocolo de negociación (handsake) negocia las claves de sesión mediante el esquema de Diffie-Hellman (D-H) o RSA. Indique la respuesta correcta:

a) D-H anónimo es susceptible de ataques por hombre interpuesto

b) D-H efímero no requiere certificado del servidor ni del cliente

c) D-H constante no precisa certificado del cliente

d) RSA necesita la generación de un número aleatorio por el servidor que es enviado al cliente cifrado con la clave pública de éste