Navegación por la prueba de conocimiento
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15
Mostrar una página cada vez
Finalizar revisión

Comenzado el	domingo, 20 de enero de 2019, 23:26
Estado	Finalizado
Finalizado en	domingo, 20 de enero de 2019, 23:28
Tiempo empleado	2 minutos 27 s
La puntuación	4,00/15,00
Calificación	**2,67** de 10,00 (**27**%)

Pregunta 1
Incorrecta
Puntúa 0,00 sobre 1,00
Marcar pregunta

¿Qué es la criptografía?

Selecciona una:
- a. Ciencia que estudia cómo romper los textos cifrados
- b. Ciencia que estudia cómo mantener la seguridad en los mensajes
- c. Ciencia que estudia cómo ocultar mensajes u objetos dentro de otros objetos (p.ej. imágenes)
- d. Ciencia que estudia cómo analizar mensajes cifrados ✗

La respuesta correcta es: Ciencia que estudia cómo mantener la seguridad en los mensajes

Pregunta 2
Correcta
Puntúa 1,00 sobre 1,00
Marcar pregunta

¿En qué consiste el cifrado César en el alfabeto español?

Selecciona una:
- a. Cada carácter de texto en claro se reemplaza por el carácter tercero a la derecha, módulo 27 ✓
- b. Asigna a un símbolo del alfabeto fuente varios del alfabeto cifrado
- c. El texto en claro se escribe como secuencia de filas (con una cierta profundidad) y se lee como secuencia de columnas
- d. Se Hace uso del disco de Alberti junto con nomenclátores

La respuesta correcta es: Cada carácter de texto en claro se reemplaza por el carácter tercero a la derecha, módulo 27

Pregunta 3
Incorrecta
Puntúa 0,00 sobre 1,00
Marcar pregunta

¿Qué problemática resuelve el uso de claves secretas K con respecto a los algoritmos de cifrado "clásicos"?

Selecciona una:
- a. Hace que Alice pueda utilizar el mismo algoritmo E en sus comunicaciones con todos los usuarios ✗
- b. Evita el "security by obscurity": Ya no es necesario mantener en secreto el algoritmo de (des)cifrado
- c. Todo lo anterior
- d. En comparación con los algoritmos de cifrado clásico, es más escalable, ya que no hace falta usar un algoritmo de cifrado para cada destinatario.

La respuesta correcta es: Todo lo anterior

Pregunta 4
Correcta
Puntúa 1,00 sobre 1,00
Marcar pregunta

¿Cuántas etapas tiene la operación de cifrado de DES?

Selecciona una:
- a. 12
- b. 16 ✓
- c. 18
- d. 20

La respuesta correcta es: 16

Pregunta 5
Incorrecta
Puntúa 0,00 sobre 1,00
Marcar pregunta

¿Cuáles son las propiedades definidas por Claude Shannon para evitar (o dificultar) los ataques basados en análisis estadísticos?

Selecciona una:
- a. Difusión y Diseminación
- b. Confusión y Permutación ✗
- c. Difusión y Confusión
- d. Permutación y Diseminación

La respuesta correcta es: Difusión y Confusión

Pregunta 6
Incorrecta
Puntúa 0,00 sobre 1,00
Marcar pregunta

¿Cuáles son las operaciones primitivas del proceso de cifrado/descifrado AES?

Selecciona una:
- a. AddRoundKey, SubBytes, ShiftRows, MixColumns
- b. XOR, S-Box ✗
- c. Rotword, SubBytes, XOR, Rcon
- d. ShiftLeft, ShiftRight, MoveRows, MoveColumns

La respuesta correcta es: AddRoundKey, SubBytes, ShiftRows, MixColumns

Pregunta 7
Incorrecta
Puntúa 0,00 sobre 1,00
Marcar pregunta

¿Qué modo de operación simula un cifrado en flujo, y proporciona tanto cifrado como autenticación?

Selecciona una:
- a. CFB
- b. CTR ✗
- c. OFB
- d. GCM

La respuesta correcta es: GCM

Pregunta 8
Correcta
Puntúa 1,00 sobre 1,00
Marcar pregunta

¿Cuáles son las tres funcionalidades básicas con la criptografía asimétrica?

Selecciona una:
- a. Póker mental, "bit commitment", ZKP
- b. Cifrado, Descifrado, Intercambio de claves
- c. Cifrado, Firma Digital, Intercambio de claves ✓
- d. Cifrado, Firma Digital, Control de acceso

La respuesta correcta es: Cifrado, Firma Digital, Intercambio de claves

Pregunta 9
Incorrecta
Puntúa 0,00 sobre 1,00
Marcar pregunta

¿En qué problema matemático se basa el protocolo Diffie Hellman original de 1976?

Selecciona una:
- a. La dificultad de computar logaritmos discretos
- b. Hallar la factorización del producto de dos números primos
- c. Encontrar el logaritmo discreto de un elemento de curva elíptica aleatoria, con respecto a un punto base conocido públicamente ✗
- d. Todo lo anterior

La respuesta correcta es: La dificultad de computar logaritmos discretos

Pregunta 10
Incorrecta
Puntúa 0,00 sobre 1,00
Marcar pregunta

¿Cuál es la forma de escoger la clave pública en el algoritmo RSA?

Selecciona una:
- a. MCD (e, PHI(n)) = 1; siendo e < PHI(n)
- b. e * d = 1 (mod PHI(n)); siendo d < PHI(n) ✗
- c. PHI(n) = (p - 1) * (q - 1)
- d. (alpha)^(Xa*Xb) mod q

La respuesta correcta es: MCD (e, PHI(n)) = 1; siendo e < PHI(n)

Pregunta 11
Incorrecta
Puntúa 0,00 sobre 1,00
Marcar pregunta

¿Cuáles son las longitudes de clave en RSA?

Selecciona una:
- a. Entre 1024 y 2048 bits, aunque puede llegar a ser 4096
- b. Entre 128 y 256 bits
- c. Entre 4096 y 16384 bits
- d. Entre 128 y 160 bits ✗

La respuesta correcta es: Entre 1024 y 2048 bits, aunque puede llegar a ser 4096

Pregunta 12
Incorrecta
Puntúa 0,00 sobre 1,00
Marcar pregunta

En una función hash criptográfica, ¿Qué significa ser "weak collision resistant" (resistencia débil a colisiones)?

Selecciona una:
- a. Para cualquier bloque x, es computacionalmente imposible encontrar una y != x tal que H(y) = H(x)
- b. Es computacionalmente imposible encontrar un par (x,y) tal que H(y) = H(x)
- c. Para una huella digital h, es computacionalmente imposible encontrar una y tal que H(y) = h ✗
- d. La función H proporciona un valor pseudoaleatorio

La respuesta correcta es: Para cualquier bloque x, es computacionalmente imposible encontrar una y != x tal que H(y) = H(x)

Pregunta 13
Incorrecta
Puntúa 0,00 sobre 1,00
Marcar pregunta

¿Cuáles funciones hash son a día de hoy seguras de utilizar?

Selecciona una:
- a. MD5 ✗
- b. SHA-1, SHA-2
- c. SHA-2, SHA-3
- d. SHA-1, Keccak

La respuesta correcta es: SHA-2, SHA-3

Pregunta 14
Incorrecta
Puntúa 0,00 sobre 1,00
Marcar pregunta

¿Qué es una función MAC?

Selecciona una:
- a. Una función que toma como entrada un mensaje M y una clave asimétrica privada Kpr, y produce un valor hash
- b. Una función que toma como entrada un mensaje M y una clave simétrica K, y produce un valor hash
- c. Una función que toma como entrada un mensaje M y una clave asimétrica pública Kpb, y produce un valor hash
- d. Una función que toma como entrada un mensaje M y un one-time-pad, y produce un valor hash ✗

La respuesta correcta es: Una función que toma como entrada un mensaje M y una clave simétrica K, y produce un valor hash

Pregunta 15
Correcta
Puntúa 1,00 sobre 1,00
Marcar pregunta

¿Qué operaciones utilizarías para descifrar el siguiente dato? Cifrado(Padding(Hash(dato)))

Selecciona una:
- a. Descifrado, Unpadding, Unhashing
- b. Descifrado con la clave privada
- c. Descifrado, Unpadding ✓
- d. Descifrado con la clave pública

La respuesta correcta es: Descifrado, Unpadding

Finalizar revisión