Navegación por la prueba de conocimiento

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20

Mostrar una página cada vez
Finalizar revisión

Comenzado el	domingo, 20 de enero de 2019, 23:30
Estado	Finalizado
Finalizado en	domingo, 20 de enero de 2019, 23:31
Tiempo empleado	1 minuto 28 s
La puntuación	6,00/20,00
Calificación	**3,00** de 10,00 (**30**%)

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

¿Qué protocolos permiten la distribución de una clave de sesión cuando la criptografía de clave pública no puede utilizarse?

Selecciona una:
- a. El protocolo Diffie Hellman
- b. Los protocolos de distribución centralizada de claves ✔
- c. Los protocolos de computación segura multiparte
- d. El protocolo SSL/TLS

La respuesta correcta es: Los protocolos de distribución centralizada de claves

Pregunta 2
Incorrecta
Puntúa 0,00 sobre 1,00
Marcar pregunta

¿Qué es el modelo PUSH?

Selecciona una:
- a. Los protocolos utilizados para revocar claves de sesión
- b. Los protocolos donde una entidad A contacta con un KDC primero antes de comunicarse con B
- c. Los protocolos donde una entidad A contacta primero con B, el cual contactará con el KDC ✘
- d. Los protocolos donde una entidad A contacta con un KDC y con B al mismo tiempo

La respuesta correcta es: Los protocolos donde una entidad A contacta con un KDC primero antes de comunicarse con B

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

¿Qué tienen en común el protocolo Needham-Schroeder y el protocolo Kerberos?

Selecciona una:
- a. Son protocolos PUSH
- b. Son protocolos PULL
- c. Son protocolos KDC
- d. Son protocolos que usan timestamps ✘

La respuesta correcta es: Son protocolos PUSH

Pregunta 4
Incorrecta
Puntúa 0,00 sobre 1,00
Marcar pregunta

¿Qué información relevante puede contener un certificado digital?

Selecciona una:
- a. La identidad del usuario, la fecha de emisión y expiración, la clave de sesión a utilizar ✘
- b. La identidad del usuario, la fecha de emisión y expiración, la clave privada del usuario
- c. La identidad del usuario, la fecha de emisión y expiración, la firma digital de quien emite el documento
- d. La identidad del usuario, la fecha de emisión y expiración, la firma digital del usuario

La respuesta correcta es: La identidad del usuario, la fecha de emisión y expiración, la firma digital de quien emite el documento

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

¿Cuál es la estructura estándar de certificado digital que ha sido adoptada internacionalmente?

Selecciona una:
- a. X.501
- b. X.509
- c. C.501 ✘
- d. C.509

La respuesta correcta es: X.509

Pregunta 6
Correcta
Puntúa 1,00 sobre 1,00
Marcar pregunta

¿Cuáles pueden ser los servicios ofrecidos por una PKI?

Selecciona una:
- a. Emisión de Certificados, Distribución de Certificados
- b. Obtención de Certificados, Certificación Cruzada
- c. Salvaguarda y Recuperación de Claves, Revocación y Suspensión de Certificados
- d. Todos los anteriores ✔

La respuesta correcta es: Todos los anteriores

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

¿Cuál es el objetivo del protocolo OCSP?

Selecciona una:
- a. Permite a los usuarios utilizar todos los servicios proporcionados por una CA de forma remota ✘
- b. Permite a los usuarios revocar certificados
- c. Permite a los usuarios consultar si un certificado esta revocado
- d. Permite a los usuarios enviar peticiones de creación de certificados

La respuesta correcta es: Permite a los usuarios consultar si un certificado esta revocado

Pregunta 8
Incorrecta
Puntúa 0,00 sobre 1,00
Marcar pregunta

La diferencia entre un certificado revocado y un certificado expirado:

Selecciona una:
- a. Un certificado revocado: se puede seguir aplicando; un certificado expirado: está completamente eliminado
- b. Un certificado revocado: no se puede seguir aplicando; un certificado expirado: está completamente eliminado ✘
- c. Un certificado revocado y un certificado expirado: ambos están completamente eliminados y no se pueden aplicar
- d. Un certificado revocado: no existe el concepto; un certificado expirado: no se puede usar

La respuesta correcta es: Un certificado revocado: se puede seguir aplicando; un certificado expirado: está completamente eliminado

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

CSR consiste en:

Selecciona una:
- a. Una solicitud de certificado emitido por una entidad para ser firmada por un CA
- b. Un certificado firmado por una CA
- c. Un certificado autofirmado ✘
- d. Una solicitud de certificado emitido por una CA

La respuesta correcta es: Una solicitud de certificado emitido por una entidad para ser firmada por un CA

Pregunta 10
Correcta
Puntúa 1,00 sobre 1,00
Marcar pregunta

Un certificado se verifica de la siguiente forma:

Selecciona una:
- a. Datos --> Hash(Datos) = EkpubCA(H(Datos)) ✔
- b. CSR --> Hash(CSR) = EkpubCA(H(CSR))
- c. CTR --> Hash(CTR) = EkpubCA(H(CTR))
- d. EprivCA(Hash(CSR)) = EkpubCA(H(CSR))

La respuesta correcta es: Datos --> Hash(Datos) = EkpubCA(H(Datos))

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

¿Qué es la "zona de seguridad" del DNI electrónico?

Selecciona una:
- a. Una zona de la memoria EEPROM que es accesible sin restricciones
- b. Una zona de la memoria EEPROM accesible por el ciudadano mediante la utilización de su PIN
- c. Una zona de la memoria EEPROM accesible por el ciudadano de forma exclusiva en los puntos de actualización del DNI-e
- d. Una zona de la memoria EEPROM que contiene el certificado de autenticación y el certificado de firma ✘

La respuesta correcta es: Una zona de la memoria EEPROM accesible por el ciudadano de forma exclusiva en los puntos de actualización del DNI-e

Pregunta 12
Correcta
Puntúa 1,00 sobre 1,00
Marcar pregunta

¿Cuál es la principal desventaja del "Single Sign-On"?

Selecciona una:
- a. El usuario debe memorizar al menos N contraseñas para N servicios
- b. Hay un único punto de ataque, el servidor SSO ✔
- c. El servidor SSO debe estar desplegado en la nube
- d. El servidor SSO tiene que implementar la tecnología Blockchain

La respuesta correcta es: Hay un único punto de ataque, el servidor SSO

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

El paso: "Trent genera un mensaje con un timestamp (Time), un tiempo de vida (L), una clave de sesión aleatoria, y la identidad de Alice. Lo cifra con la clave compartida con Bob. Prepara un mensaje similar para Alice. Envía ambos mensajes cifrados a Alice." Lo ejecuta:

Selecciona una:
- a. Kerberos
- b. Otway-Rees
- c. Needham-Schroeder ✘
- d. Kao Chow

La respuesta correcta es: Kerberos

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

¿Qué es el servicio de auditoría?

Selecciona una:
- a. La concesión de un derecho o un permiso a una entidad para acceder a un recurso
- b. La prevención de los accesos a recursos por parte de usuarios no autorizados
- c. La implantación de las políticas de seguridad ✘
- d. La revisión de los registros y actividades del sistema para, por ejemplo, comprobar la adecuación de los sistemas de control

La respuesta correcta es: La revisión de los registros y actividades del sistema para, por ejemplo, comprobar la adecuación de los sistemas de control

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

Dada la siguiente ACL: autoexec.bat = {(Rodrigo, {r}); (Ramon, {rw}); (Cristina, {rwx}); (Javier, {rx})}, ¿Quién puede escribir (w) en el fichero autoexec.bat?

Selecciona una:
- a. Ramon y Cristina ✔
- b. Rodrigo y Cristina
- c. Rodrigo y Ramon
- d. Ramon y Javier

La respuesta correcta es: Ramon y Cristina

Pregunta 16
Incorrecta
Puntúa 0,00 sobre 1,00
Marcar pregunta

¿Cuáles son las entidades del modelo RBAC?

Selecciona una:
- a. Usuario, rol y permiso
- b. Usuario, rol, permiso y sesión
- c. Usuario, rol, permiso y restricciones
- d. Usuario y rol ✘

La respuesta correcta es: Usuario, rol, permiso y sesión

Pregunta 17
Incorrecta
Puntúa 0,00 sobre 1,00
Marcar pregunta

¿En qué consiste el modelo CapBAC?

Selecciona una:
- a. Es un modelo que intenta mejorar el modelo RBAC en función de los flujos de trabajo de una organización
- b. Es un modelo que extiende y mejora el uso de RBAC, relacionando sujetos con roles, operaciones con actividades, y objetos con vistas. ✘
- c. Es un modelo en el que el acceso no está basado en los permisos del usuario, sino en los atributos del usuario
- d. Es un modelo en el que el acceso sólo es posible si el usuario recibe del proveedor del recurso un token, el cual posibilitará que el usuario pueda realizar determinadas acciones sobre un recurso

La respuesta correcta es: Es un modelo en el que el acceso sólo es posible si el usuario recibe del proveedor del recurso un token, el cual posibilitará que el usuario pueda realizar determinadas acciones sobre un recurso

Pregunta 18
Incorrecta
Puntúa 0,00 sobre 1,00
Marcar pregunta

¿Qué diferencia hay entre un protocolo de división de secretos y un protocolo de compartición de secretos?

Selecciona una:
- a. El protocolo de compartición de secretos es el único que hace uso de la operación XOR ✘
- b. El protocolo de compartición de secretos es el único que puede reconstruir el mensaje original si k sombras están disponibles.
- c. El protocolo de división de secretos es el único que divide el mensaje original en N sombras.
- d. El protocolo de división de secretos es el único que hace uso de polinomios de grado N.

La respuesta correcta es: El protocolo de compartición de secretos es el único que puede reconstruir el mensaje original si k sombras están disponibles.

Pregunta 19
Incorrecta
Puntúa 0,00 sobre 1,00
Marcar pregunta

El protocolo de "bit commitment", ¿con qué primitivas criptográficas puede implementarse?

Selecciona una:
- a. Funciones hash y HMAC
- b. Criptografía asimétrica y pruebas de conocimiento cero (ZKP)
- c. Criptografía simétrica y funciones hash
- d. Funciones hash y protocolos de lanzamiento de moneda ✘

La respuesta correcta es: Criptografía simétrica y funciones hash

Pregunta 20
Correcta
Puntúa 1,00 sobre 1,00
Marcar pregunta

El póker metal y el lanzamiento de moneda se aplican si el algoritmo implementando cumple la siguiente condición:

Selecciona una:
- a. DK1 (EK2 (EK1 (M))) = EK2 (M) ✔
- b. DK1 (EK1 (EK2 (M))) = EK2 (M)
- c. EK1 (DK2 (EK1 (M))) = EK2 (M)
- d. EK2 (EK1 (DK2 (M))) = EK2 (M)

La respuesta correcta es: DK1 (EK2 (EK1 (M))) = EK2 (M)

Finalizar revisión