

Navegación por la prueba de conocimiento

12345678910111213141516171819

Mostrar una página cada vez

Finalizar revisión

Comenzado el	domingo, 20 de enero de 2019, 23:32
Estado	Finalizado
Finalizado en	domingo, 20 de enero de 2019, 23:33
Tiempo empleado	1 minuto 13 s
La puntuación	3,00/19,00
Calificación	1,58 de 10,00 (16%)

Pregunta 1

Incorrecta

Puntuá 0,00 sobre 1,00

Marcar pregunta

*Eks(Zip(M)) || Kpubb(Ks)" es una operación específica de:

Selecciona una:

☐ a. PGP

☒ b. SMIME

☐ c. FTPS

☐ d. SFTP

La respuesta correcta es: PGP

Pregunta 2

Incorrecta

Puntuá 0,00 sobre 1,00

Marcar pregunta

¿Cuáles son las operaciones proporcionadas por PGP?

Selecciona una:

☐ a. Firma digital, cifrado

☐ b. Firma digital, cifrado, compresión, compatibilidad de e-mail

☒ c. Firma digital, cifrado, compresión, compatibilidad de e-mail, anonimato

☐ d. Firma digital, compresión, compatibilidad de e-mail

La respuesta correcta es: Firma digital, cifrado, compresión, compatibilidad de e-mail

Pregunta 3

Incorrecta

Puntuá 0,00 sobre 1,00

Marcar pregunta

¿Cuál es el modelo de PKI utilizado por PGP?

Selecciona una:

☒ a. Modelo de PKI jerárquico

☐ b. Modelo de PKI híbrido

☐ c. Modelo de PKI en malla

☐ d. Modelo de PKI en círculo

La respuesta correcta es: Modelo de PKI en malla

Pregunta 4

Incorrecta

Puntuá 0,00 sobre 1,00

Marcar pregunta

¿Cuál es el modelo de PKI utilizado por S/MIME?

Selecciona una:

☐ a. Modelo de PKI jerárquico

☐ b. Modelo de PKI híbrido

☐ c. Modelo de PKI en malla

☒ d. Modelo de PKI en círculo

La respuesta correcta es: Modelo de PKI híbrido

Pregunta 5

Incorrecta

Puntuá 0,00 sobre 1,00

Marcar pregunta

¿Dónde se realiza el cifrado en el protocolo SSH?

Selecciona una:

☒ a. En la capa física

☐ b. En la capa de red

☐ c. En la capa de transporte

☐ d. En la capa de aplicación

La respuesta correcta es: En la capa de aplicación

Pregunta 6

Incorrecta

Puntuá 0,00 sobre 1,00

Marcar pregunta

¿Cómo se pueden clasificar los sistemas de pagos electrónicos?

Selecciona una:

☐ a. Según el momento en el que el vendedor contacta con el banco

☐ b. Según el momento en que se retira el dinero de la cuenta del comprador

☒ c. Según la cantidad implicada en la transacción

☐ d. Todos los anteriores

La respuesta correcta es: Todos los anteriores

Pregunta 7

Incorrecta

Puntuá 0,00 sobre 1,00

Marcar pregunta

SET asegura:

Selecciona una:

☐ a. Confidencialidad, autenticidad, privacidad, integridad y no-repudio

☒ b. Confidencialidad, autenticidad, privacidad, integridad y repudio

☐ c. Confidencialidad, autenticidad, integridad y repudio

☐ d. Confidencialidad, autenticidad y no-repudio

La respuesta correcta es: Confidencialidad, autenticidad, privacidad, integridad y no-repudio

Pregunta 8

Incorrecta

Puntuá 0,00 sobre 1,00

Marcar pregunta

¿Cuál es el objetivo principal de la firma dual?

Selecciona una:

☐ a. Ocultar el mensaje de pago y el mensaje del pedido

☐ b. Enlazar dos mensajes que han de ir a receptores diferentes

☒ c. Encadenar varios hashes de la siguiente forma: H(H(00)||H(P1))

☐ d. Involucrar a una tercera parte confiable en el protocolo

La respuesta correcta es: Enlazar dos mensajes que han de ir a receptores diferentes

Pregunta 9

Incorrecta

Puntuá 0,00 sobre 1,00

Marcar pregunta

¿Cuál era la principal base tecnológica de Cybercash, que luego se utilizó en Paypal?

Selecciona una:

☐ a. La integración de una pasarela de pago

☐ b. El uso de criptografía de clave pública

☐ c. La implementación de sistemas de micropago para crear servicios como Patreon

☒ d. El uso de modelos de PKI en malla

La respuesta correcta es: La integración de una pasarela de pago

Pregunta 10

Incorrecta

Puntuá 0,00 sobre 1,00

Marcar pregunta

¿Qué es el "Anonimato no rastreado"?

Selecciona una:

☒ a. El que implementa pseudónimos donde la identidad del usuario original se "comparte" entre dos o más partes implicadas

☐ b. El que únicamente se basa de técnicas para ocultar la identidad de un usuario a través de pseudónimos

☐ c. El que garantiza que la identidad de los usuarios no se puede revelar, y que el conjunto de las operaciones realizadas por un usuario anónimo no se puedan vincular

☐ d. El que implementa técnicas mucho más estrictas desde el punto de vista a la privacidad del usuario para evitar su rastreo

La respuesta correcta es: El que implementa técnicas mucho más estrictas desde el punto de vista a la privacidad del usuario para evitar su rastreo

Pregunta 11

Incorrecta

Puntuá 0,00 sobre 1,00

Marcar pregunta

"la incapacidad de un atacante para relacionar dos mensajes o entidades observadas" corresponde a:

Selecciona una:

☐ a. no-vinculación

☐ b. anonimato

☒ c. no-observación

☐ d. anonimato no rastreado

La respuesta correcta es: no-vinculación

Pregunta 12

Incorrecta

Puntuá 0,00 sobre 1,00

Marcar pregunta

¿Cuál es la característica principal de la firma en anillo?

Selecciona una:

☐ a. Cualquier miembro del grupo firma mensajes de forma completamente anónima en nombre del grupo

☒ b. Cualquier miembro del grupo firma mensajes de forma parcialmente anónima en nombre del grupo

☐ c. El firmante firma mensajes para otros usuarios, pero desconoce el contenido de los mensajes que firma

☐ d. La firma la producen conjuntamente un mínimo de t usuarios, en nombre del grupo de n usuarios (t < n) del que forman parte

La respuesta correcta es: Cualquier miembro del grupo firma mensajes de forma completamente anónima en nombre del grupo

Pregunta 13

Incorrecta

Puntuá 0,00 sobre 1,00

Marcar pregunta

La apertura de una firma de grupo consiste en:

Selecciona una:

☐ a. Devolver la ID del miembro que realizó la firma y una prueba de ello

☐ b. Devolver el mensaje firmado y una prueba del hecho

☐ c. Devolver la ID del miembro que realizó la firma y el mensaje firmado

☒ d. Devolver el mensaje firmado y un nonce asociado a la firma

La respuesta correcta es: Devolver la ID del miembro que realizó la firma y una prueba de ello

Pregunta 14

Correcta

Puntuá 1,00 sobre 1,00

Marcar pregunta

La firma ciega se basa en:

Selecciona una:

☒ a. M' = M.r^e mod n

☐ b. M' = M.r^d mod n

☐ c. M' = M.r^(de) mod n

☐ d. M' = M.r^(n-1) mod n

La respuesta correcta es: M' = M.r^e mod n

Pregunta 15

Incorrecta

Puntuá 0,00 sobre 1,00

Marcar pregunta

Selecciona ejemplos de las propiedades o condiciones iniciales que debe satisfacer un esquema de firma de grupo

Selecciona una:

☐ a. Un grupo k de miembros del grupo pueden conocer qué miembro del grupo ha firmado el mensaje

☐ b. Los miembros no pueden evitar la apertura de la firma por parte del administrador, ni firmar por otro

☐ c. El miembro firmante no puede conocer el contenido del mensaje

☒ d. Todas las anteriores

La respuesta correcta es: Los miembros no pueden evitar la apertura de la firma por parte del administrador, ni firmar por otro

Pregunta 16

Correcta

Puntuá 1,00 sobre 1,00

Marcar pregunta

Algunos protocolos de privacidad siguen arquitecturas descentralizadas como:

Selecciona una:

☒ a. Crowds y Hordes

☐ b. Mix-nets y Hordes

☐ c. Crowds y TOR

☐ d. Hordes y TOR

La respuesta correcta es: Crowds y Hordes

Pregunta 17

Incorrecta

Puntuá 0,00 sobre 1,00

Marcar pregunta

¿Cómo es una solución de privacidad basada en un proxy?

Selecciona una:

☐ a. Varios servidores se agrupan, y todos enrutan los paquetes aleatoriamente los paquetes recibidos de sus compañeros

☒ b. Un servidor crea un paquete cifrado en capas, que se irán "pelando" a medida que atraviese el camino

☐ c. Un servidor almacena las comunicaciones de varios clientes, y las envía mezcladas

☐ d. Un servidor hace de intermediario en la comunicación, aceptando conexiones de los clientes y reenviándolas

La respuesta correcta es: Un servidor hace de intermediario en la comunicación, aceptando conexiones de los clientes y reenviándolas

Pregunta 18

Incorrecta

Puntuá 0,00 sobre 1,00

Marcar pregunta

En una conexión TOR, ¿dónde se encuentra la conexión no cifrada?

Selecciona una:

☐ a. Entre el origen y el segundo nodo del canal de comunicaciones

☐ b. Entre el penúltimo nodo del canal de comunicaciones y el destino

☐ c. Todas las comunicaciones se encuentran "en abierto"

☒ d. Todas las conexiones se encuentran cifradas

La respuesta correcta es: Entre el penúltimo nodo del canal de comunicaciones y el destino

Pregunta 19

Correcta

Puntuá 1,00 sobre 1,00

Marcar pregunta

Si en TOR la ruta a tomar es: R2 -> R3 -> R15 -> R17, entonces la comunicación se debería proteger de la siguiente forma:

Selecciona una:

☒ a. KpubR2(KpubR3(KpubR15(KpubR17(M))))

☐ b. KpubR17(KpubR15(KpubR3(KpubR2(M))))

☐ c. KpubR2(KpubR3(KpubR17(KpubR15(M))))

☐ d. KpubR17(KpubR3(KpubR15(KpubR2(M))))

La respuesta correcta es: KpubR2(KpubR3(KpubR15(KpubR17(M))))