

Comenzado el	jueves, 25 de abril de 2024, 11:40
Estado	Finalizado
Finalizado en	miércoles, 1 de mayo de 2024, 13:50
Tiempo empleado	6 días 2 horas
Calificación	10,00 de 10,00 (100%)

Pregunta 1

Correcta

Se puntúa 0,50 sobre 0,50

El esquema AAA debe este nombre a las palabras:

Seleccione una:

- ☐ a. Amenaza, Ataque y Autenticación
- ☐ b. Autenticación, Autorización y Anonimato
- ☐ c. Ninguna de las anteriores
- ☒ d. Autenticación, Autorización y Auditoría ✓

Respuesta correcta

La respuesta correcta es: Autenticación, Autorización y Auditoría

Pregunta 2

Correcta

Se puntúa 1,00 sobre 1,00

Según el protocolo de Feige-Fiat-Shamir, ¿cuál/es de las siguiente/s respuestas es incorrecta?

Seleccione una:

- ☐ a. $n=39, s=5, v_1=25, r=7, s=+1, x=10, a_1=1, y=35$
- ☒ b. $n=35, s_1=7, v_1=14, r=6, s=+1, x=1, a_1=0, y=6$ ✓ $s_1=7$ no es primo con $n=35$
- ☐ c. $n=77, s_1=9, v_1=4, r=6, s=-1, x=-36, a_1=1, y=54$
- ☐ d. $n=39, s=8, v_1=25, r=5, s=-1, x=-25, a_1=0, y=5$

Respuesta correcta

La respuesta correcta es: $n=35, s_1=7, v_1=14, r=6, s=+1, x=1, a_1=0, y=6$

Pregunta 3

Correcta

Se puntúa 1,00 sobre 1,00

Alice envía a Bob el mensaje cifrado con RSA, $C=37$, siendo los parámetros de ambos participantes los siguientes:

$n_A=143$, $e_A=7$, $n_B=69$, $e_B=5$

Sabiendo que $p_A=13$, $q_A=11$, $p_B=23$, $q_B=3$, obtén el descifrado del mensaje

Respuesta: 

La respuesta correcta es: 67


Pregunta 4

Correcta

Se puntúa 1,00 sobre 1,00

En el esquema de S/KEY, ¿qué no es cierto?

Seleccione una:

- ☒ a. El servidor almacena todas las contraseñas cifradas 
- ☐ b. El usuario utiliza como primera contraseña de acceso la penúltima contraseña generada
- ☐ c. El usuario almacena, o puede calcular, todas las contraseñas
- ☐ d. La generación de las contraseñas consiste en la aplicación sucesiva de una función hash

Respuesta correcta

La respuesta correcta es: El servidor almacena todas las contraseñas cifradas


Pregunta 5

Correcta

Se puntúa 1,00 sobre 1,00

¿Cuál de los siguientes no es un método de revocación de certificados?

Seleccione una:

- ☐ a. Todos son métodos de revocación de certificados
- ☒ b. X.509 
- ☐ c. CRL
- ☐ d. OCSP

Respuesta correcta

La respuesta correcta es: X.509

Pregunta 6

Correcta

Se puntúa 1,00 sobre 1,00

Si Alice envía a Bob un mensaje M cuyo mensaje resumido es $h(M)=11$, firmado con la firma RSA 132, siendo sus parámetros $n_A=143$, $n_B=69$, $d_A=7$, $d_B=5$, $e_A=103$, $e_B=5$

¿Bob acepta esta firma como válida?

Seleccione una:

- ☒ Verdadero ✓
- ☐ Falso

La respuesta correcta es 'Verdadero'

Pregunta 7

Correcta

Se puntúa 1,00 sobre 1,00

Determinar la firma RSA **de Alice** para el mensaje ARMA, **que envía a Bob** sabiendo que $(n_B, e_B) = (2947, 179)$, $(n_A, e_A) = (2773, 157)$ $d_B = 1619$ y $d_A = 17$.

En este caso, las letras A, ..., Z del alfabeto se codifican con 0, ..., 25, el punto es el 26 y el espacio en blanco es el 27.

Introducir sólo el primer valor de la respuesta.

Respuesta: 1071



La respuesta correcta es: 1071

Pregunta 8

Correcta

Se puntúa 1,00 sobre 1,00

Si Alice cifra el mensaje $m=16$ con el criptosistema de ElGamal para enviarlo a Bob, quien utiliza como clave pública $(p, a^x \pmod p)$, $a=23$, $p=19$, ¿cuál de las siguientes parejas $\{K,C\}$ es correcta?

Seleccione una:

- ☐ a. $\{22, 11\}$
- ☐ b. $\{10, 11\}$
- ☒ c. $\{16, 3\}$ ✓
- ☐ d. $\{11, 10\}$

La respuesta correcta es: $\{16, 3\}$

Pregunta 9

Correcta

Se puntúa 1,00 sobre 1,00

Sobre SHA, ¿qué no es cierto?

Seleccione una:

- ☐ a. SHA son las siglas de Secure Hash Algorithm
- ☐ b. SHA-0 y SHA-1 producen una salida de 160 bits de un mensaje que puede tener un tamaño máximo de 264 bits
- ☐ c. SHA-3 es la actual función hash standard
- ☒ d. Todas las funciones hash denominadas SHA son similares a MD5 ✓
- ☐ e. Se conoce como SHA-2 a las cuatro variantes SHA-224, SHA-256, SHA-384, y SHA-512.
- ☐ f. La primera versión se denota a veces SHA-0
- ☐ g. SHA-3 antes se llamaba Keccak
- ☐ h. SHA es una familia de funciones hash de la NSA de EEUU publicadas por el NIST

Respuesta correcta

La respuesta correcta es: Todas las funciones hash denominadas SHA son similares a MD5

Pregunta 10

Correcta

Se puntúa 0,50 sobre 0,50

¿Cuál/es de los siguientes cifrados se usa/n en TLS 1.3?

Seleccione una o más de una:

- ☐ a. Snow3G
- ☒ b. ChaCha20 ✓
- ☐ c. RC4
- ☐ d. DES
- ☒ e. AES ✓

Respuesta correcta

Las respuestas correctas son: ChaCha20, AES

Pregunta 11

Correcta

Se puntúa 1,00 sobre 1,00

De las siguientes, la forma más insegura de demostrar la autenticidad de la identidad del usuario es en base a:

Seleccione una:

- ☐ a. varios factores combinados
- ☒ b. algo que se sabe ✓
- ☐ c. algo que se posee
- ☐ d. alguna característica física

Respuesta correcta

La respuesta correcta es: algo que se sabe