Comenzado el	martes, 24 de enero de 2023, 13:00
Estado	Finalizado
Finalizado en	martes, 24 de enero de 2023, 13:00
Tiempo empleado	14 segundos

Pregunta **1**

Sin contestar

Puntúa como 1,00

¿Qué longitud mínima de clave se recomienda en criptosistemas de clave pública basados en la dificultad de calcular logaritmos discretos en $\mathbb{Z}_p^*$?

Seleccione una:

a. El doble que en RSA.

b. Igual que en RSA.

c. La mitad que en RSA.

La respuesta correcta es: Igual que en RSA.

Pregunta **2**

Sin contestar

Puntúa como 1,00

Un usuario cuya clave pública es el punto de la curva ANSI X9.62 elliptic curve secp384r1 (NIST P-384):
(215546959578002304535783617935541478626699039318911357522180346325024665194018611237476172
203271296450244627905211109053998248567316303553747086451349434273526590333432676625757361 25

ha firmado un documento con hash:
127545251311822701649065144790946222842257619912280432522432524706214842040422439008982545 13

obteniendo la firma:
(132637519456546894288183203492543525236653838682320331277972047776413683787962662360300715 8
321463584860646921399839111429547692620845045131194500367182893857379977609019241956073891 45

Seleccione una:

Falso

Cierto

La respuesta correcta es: Cierto

Pregunta **3**

Sin contestar

Puntúa como 1,00

Un algoritmo para resolver el problema del logaritmo discreto puede usarse para resolver el problema de Diffie-Hellman

Seleccione una:

- Verdadero
- Falso

La respuesta correcta es 'Verdadero'

Pregunta **4**

Sin contestar

Puntúa como 1,00

Un usuario cuya clave pública es un punto de la curva ANSI X9.62 elliptic curve secp521r1 (NIST P-521) ha firmado dos documentos usando el mismo número aleatorio. Los resultados son:

Hash del primer mensaje:
0xb565aed85c06be130291043bae2b1b07d365a6a20639c23af7e28c28475845735293a4aa0fb2d6c8ce39495f6cb9

Primera firma:
(391144904089596930229938933529512509579736362743698072377604694439035632514180766146736188
459844920873766703382450906361052003873104206851722710308528347888243068218079892293657649 43

Hash del segundo mensaje:
0x27e4034d4ec68d5e00effb471f36846bb23b047b6aac2f553a19f453b64f3383bd4e0dce544d207ebf70026c720f3b

Segunda firma:
(391144904089596930229938933529512509579736362743698072377604694439035632514180766146736188
445910942527002662720832798702836752745772067971401268388357669939413740210254187866578306 19

Calcula su clave privada.

Respuesta:

La respuesta correcta es: 555555555555555522222222233333333332222222222

Pregunta **5**

Sin contestar

Puntúa como 1,00

OCSP

Seleccione una:

a. es un protocolo para determinar el estado de un certificado en cada momento.

b. es un protocolo para buscar certificados

b. es un protocolo para buscar certificados.

c. es un protocolo para revocar certificados.

La respuesta correcta es: es un protocolo para determinar el estado de un certificado en cada momento.

Pregunta **6**

Sin contestar

Puntúa como 1,00

++

Block:

previous_block_hash:
312242924808911849479051425103604997481886996854157223258323582102268035232

block_hash: 32913054361703563669153793576202057517067728388035989298541810241209692097

seed: 3141683475901211307547989473453913452684045358938510538598389160685116442738799022

transaction:

.....

publicExponent: 65537,

modulus:
176092757188977057976939449277492878880982446706681237406390717546453106231294811634561571 75

message: 749782854256735267277446180337079278256264443979795622610622638467039915212 32

signature:
630671446259708694386416642899719575624604758481856335662438871160529326551200464327062136 37

.....

***Proof of work/dificultad* d=8**

Seleccione una:

a. Ni la transacció ni el hash són correctes.

b. El bloc és correcte.

c. El hash del bloc no és correcte pero la transacció sí.

d. La transacció no és correcta però el hash sí.

La respuesta correcta es: El hash del bloc no és correcte pero la transacció sí.

Pregunta **7**

Sin contestar

Puntúa como 1,00

¿Qué ventaja tiene usar el teorema chino de los restos al descifrar y firmar con el RSA?

Seleccione una:

- No es necesario conocer p y q.
- Ninguna.
- Permite hacer las operaciones más costosas módulo p y q en vez de módulo $n = p\,q$.

La respuesta correcta es: Permite hacer las operaciones más costosas módulo p y q en vez de módulo $n = p\,q$.

Pregunta **8**

Sin contestar

Puntúa como 1,00

Una CRL

Seleccione una:

- a. es una lista de certificados válidos.
- b. es una lista de certificados caducados.
- c. es una lista de certificados revocados.

La respuesta correcta es: es una lista de certificados revocados.

Pregunta **9**

Sin contestar

Puntúa como 1,00

Nota: Aunque en este cuatrimestre no se ha explicado, podéis encontrar cómo resolverlo en el notebook del RSA.

En una corporación se ha decidido que los usuarios compartan el módulo n.

Se ha enviado el mismo mensaje m cifrado usando RSA, $c \equiv m^e \mod n$, a dos usuarios diferente de dicha corporación.

El usuario A con clave
$(e, n) = (443, 122089277670347173171607547816668187071730015942892952856703286447766223$
ha recibido
$c = 660601233489735653420630958420468554625698036808413997357732052337105929386953 18$

El usuario B con clave

$(e, n) = (367, 122089277670347173171607547816668187071730015942892952856703286447766223$
ha recibido
$c = 930444039837387243264194051560088707461551472156203690502378401060922803211690025$

Halla el mensaje m.

Respuesta:

La respuesta correcta es:
777777777777777777777777777777733333333333333333333333333333333333333399999999999999999999

◄ Test clave pública

Ir a...

Examen final ►