Començat el	divendres, 2 de desembre 2022, 19:04
Estat	Acabat
Completat el	dilluns, 5 de desembre 2022, 10:33
Temps emprat	2 dies 15 hores

Pregunta **1**

No s'ha respost

Puntuat sobre 1,00

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

Trieu-ne una:

- Vertader
- Fals

La resposta correcta és 'Vertader'.

Pregunta **2**

No s'ha respost

Puntuat sobre 1,00

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

Trieu-ne una:

- a. El doble que en RSA.
- b. La mitad que en RSA.
- c. Igual que en RSA.

La resposta correcta és: Igual que en RSA.

Pregunta **3**

No s'ha respost

Puntuat sobre 1,00

OCSP

Trieu-ne una:

- a. es un protocolo para determinar el estado de un certificado en cada momento.
- b. es un protocolo para revocar certificados.
- c. es un protocolo para buscar certificados.

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

Pregunta **4**

No s'ha respost

Puntuat sobre 1,00

Una CRL

Trieu-ne una:

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

La resposta correcta és: es una lista de certificados revocados.

Pregunta **5**

Incorrecte

Puntuat sobre 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:
0xb565aed85c06be130291043bae2b1b07d365a6a20639c23af7e28c28475845735293a4aa0fb2d6c8ce39495f6cb996bf50644c0a5cfdf87b9c0e5

Primera firma:
(391144904089596930229938933529512509579736362743698072377604694439035632514180766146736188189167502267095737638196
459844920873766703382450906361052003873104206851722710308528347888243068218079892293657649436262514099218164195342 9

Hash del segundo mensaje:
0x27e4034d4ec68d5e00effb471f36846bb23b047b6aac2f553a19f453b64f3383bd4e0dce544d207ebf70026c720f3b287be10813677f572377def2(

Segunda firma:
(391144904089596930229938933529512509579736362743698072377604694439035632514180766146736188189167502267095737638196
445910942527002662720832798702836752745772067971401268388357669939413740210254187866578306198066189169492956604056 4

Calcula su clave privada.

Resposta: 1897292291824391620728744654188009731041681841217214087868811602467791140519927 37 ✖

La resposta correcta és: 55555555555555552222222223333333333222222222 2

Pregunta **6**

No s'ha respost

Puntuat sobre 1,00

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

Trieu-ne una:

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

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

Pregunta **7**

No s'ha respost

Puntuat sobre 1,00

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

Un usuario cuya clave pública es el punto de la curva ANSI X9.62 elliptic curve secp384r1 (NIST P-384):
(215546959578002304535783617935541478626699039318911357522180346325024665194018611237476172223441893422475262672845
203271296450244627905211109053998248567316303553747086451349434273526590333432676625757361254263194002063488983008 2

ha firmado un documento con hash:
127545251311822701649065144790946222842257619912280432522432524706214842040422439008982545135224780623399153801019 2

obteniendo la firma:
(132637519456546894288183203492543525236653838682320331277972047776413683787962662360300715895448064840550984534825
321463584860646921399839111429547692620845045131194500367182893857379977609019241956073891457588677511575888068430 3)

Trieu-ne una:

- Cierto
- Falso

La resposta correcta és: Cierto

Pregunta **8**

No s'ha respost

Puntuat sobre 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
$(e, n) = (443, 122089277670347173171607547816668187071730015942892952856703286447766223907280517077462035537$
ha recibido
$c = 660601233489735653420630958420468554625698036808413997357732052337105929386953181209096653744843007 87$

El usuario B con clave
$(e, n) = (367, 122089277670347173171607547816668187071730015942892952856703286447766223907280517077462035537$
ha recibido
$c = 930444039837387243264194051560088707461551472156203690502378401060922803211690252303251287480411056 60$

Halla el mensaje m.

Resposta:

La resposta correcta és:
777777777777777777777777777777733333333333333333333333333333333333333333399999999999999999999999999999999666666666

Pregunta **9**

No s'ha respost

Puntuat sobre 1,00

++

Block:

previous_block_hash: 31224292480891184947905142510360499748188699685415722325832358210226803523 2

block_hash: 32913054361703563669153793576202057517067728388035989298541810241209692097

seed: 31416834759012113075479894734539134526840453589385105385983891606851164427387990 22

transaction:

.....

publicExponent: 65537,

modulus:
176092757188977057976939449277492878880982446706681237406390717546453106231294811634561571751521824488595349444065 0

message: 74978285425673526727744618033707927825626444397979562261062263846703991521232

signature:
630671446259708694386416642899719575624604758481856335662438871160529326551200464327062136375731163385368640791129

.....

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

Trieu-ne una:

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

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

c. Ni la transacció ni el hash són correctes.

d. El bloc és correcte.

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

◄ Ejemplo Test clave secreta

Salta a...

Why Cryptography Is Harder Than It Looks ►