Començat el	dissabte, 16 de desembre 2023, 11:41
Estat	Acabat
Completat el	dissabte, 16 de desembre 2023, 13:00
Temps emprat	1 hora 18 minuts

Pregunta 1

Correcte

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
$(e, n) = (631, 1705383206974368725498096490668160685252783155035856136169266006582796618417940528145563105176782415184($
ha recibido
$c = 1436489107606085416296557978636692332496542901926679464493538639587187827144669136718097337698631516339719101176$

El usuario B con clave
$(e, n) = (419, 1705383206974368725498096490668160685252783155035856136169266006582796618417940528145563105176782415184($
ha recibido
$c = 7625383393969558091504388423068952283745933998925391329690044910345851680492547765324654943682580771052738383537$

Halla el mensaje m.

Resposta: 77777777777777777777777777777770000000000000000000000000000000001111111111111111

La resposta correcta és:
77777777777777777777777777777770000000000000000000000000000000011111111111111111111111111111111116666666666666666666666666666(

Pregunta 2

Correcte

Puntuat sobre 1,00

Una CRL

Trieu-ne una:

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

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

Pregunta 3

Correcte

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

La resposta correcta és: Igual que en RSA.

Pregunta 4

Incorrecte

Puntuat sobre 1,00

Un usuario cuya clave pública es un punto de la curva ANSI X9.62 elliptic curve secp384r1 (NIST P-384) ha firmado dos documentos usando el mismo número aleatorio. Los resultados son:

Hash del primer mensaje: 0x8708878e50041df55aeaf58e1ee03dc723aab45d36d47f4e1d49597b35aa6eb2f29b815b3131a4d8225610e909c4ca2f

Primera firma:
(187299736791908176231181113137718288636634835137748371524087597004449596753803954844417822810889863255680281255723 13,
203593141148943988834835802784642563228672514389425728665763245640097865232015521701000513402930966551808306249453 18)

Hash del segundo mensaje: 0x47147e25d90562e96e978cff70ff1c208a482c28ebcc45d3552d62d4eb65c45ed0a7ed1b1c8f998ad9a7240e9bf12e9

Segunda firma:
(187299736791908176231181113137718288636634835137748371524087597004449596753803954844417822810889863255680281255723 13,
335494089919982535995528539705265093753714747249842179403280173237990402050206942326607074924117773503212532434653 21)

Calcula su clave privada.

Resposta: 3545288455133239691875847822588431731058502152837530494167622051965186186839262 2 ✖

La resposta correcta és: 444444444444444422222222288888888555555555

Pregunta 5

Correcte

Puntuat sobre 1,00

Un usuario cuya clave pública es el punto de la curva ANSI X9.62 elliptic curve secp521r1 (NIST P-521):
(183746701883757124826755524715142517173684662596382931014900106779410231692051781676595944589173697763631191386590655544007103
160128187771017084884733851296769181290358318082668539230051734054120841357001260962760395416992744931611185362232547458671841 2

ha firmado un documento con hash:
557221836336932571062275534908015864296613891259449626813761978203150199311657016973349048565361003336882316515738275935362137 7

obteniendo la firma:
(636209411702914270661152765691119681822202526214190888223313780804486620649417809538075073320536552396577393606651565148805816 7
566594480202995116861238597556051114997896486779661800922955455469503961886856085705858549899405125397107024172558200907441619 2

Trieu-ne una:

- Falso ✔
- Cierto

La resposta correcta és: Falso

Pregunta 6

Correcte

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 7

Correcte

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 8

Correcte

Puntuat sobre 1,00

++
Block:
previous_block_hash: 109210143286374015256251261258669798848309832525317261534933554553012879 3
block_hash: 442305843093921801902022929707264829867840382979725486904805105115992092
seed: 721864726095922772428032239750515560994529944944679262972275736031525025949 98
.....
Transaction:
publicExponent: 65537,
modulus:
864025209863709809429564984509248606017127212834608005598252869968782127144761876392257847513000976826879113739147293018711710 5
message: 18209271279923133578
signature:
364243446180290738329481965872030735112777127547548557628888930745946302902518200081115531103333221997716884441882417846867151 1
.....

Dificultad: 16

Trieu-ne una:

- El hash del bloque no es correcto pero la transacción sí.
- El bloque es correcto.
- La transacción no es correcta pero el hash sí. ✔
- Ni la transacción ni el hash son correctos.

La resposta correcta és: La transacción no es correcta pero el hash sí.

Pregunta 9

Correcte

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 10

Correcte

Puntuat sobre 1,00

Se ha enviado el mismo mensaje m cifrado usando RSA, $c \equiv m^e \mod n$, a 5 usuarios diferentes.

El usuario A con clave
$(e, n) = (5, 11704458880696591489703356592616416025127868098410953766007322413765303922671395383720842616703077269781$
ha recibido
$c = 23811350048378972891909721245562314171188079307313240691602579566644356094643143856804692504706208311380950089$

El usuario B con clave
$(e, n) = (5, 17234261282515109030920373387929821699941371306961933980268800658182839692020822375533773555017682851968$
ha recibido
$c = 24998730933499323240232814258952964311374805230323682958555077405818608655285980287991919906650922081975095224$

El usuario C con clave
$(e, n) = (5, 19053471012090780990243272591945771901765983282293268088579846661520394095256752218097009967231753236434$
ha recibido
$c = 36324737459887927388021940524693354675055480495648757251269184239154033480436452710895354187771201413855808889$

El usuario D con clave
$(e, n) = (5, 22610770261657789496058163182213778222550168328189289540160032215867782655240728693716233181590330679713$
ha recibido
$c = 14092206206170010575015738882831596771049617709664213762145950696568424171340990992619842978683001025015736539$

El usuario E con clave
$(e, n) = (5, 21950753793319115751513988943054963225104568326742396944258659289484943230064914465252162060935004886578$
ha recibido
$c = 12270886775846611899442389328947778782582612652536625498026593376049816567444568574813082551421753150567283738$

Halla el mensaje m.

Resposta: 444444444000000000000000000008888888888833333333333444444444555555555333333333388888888888999999999999 ✔

La resposta correcta és: 444444444000000000000000000008888888888833333333333444444444555555555333333333388888888888999999999999

Pregunta 11

Parcialment correcte

Puntuat sobre 3,00

Sobre el certificado X509 (en formato PEM) siguiente se pide:

Tipo de clave:

- (•) RSA-2048 ✔
- ( ) RSA-4096
- ( ) ECC-256
- ( ) ECC-384
- ( ) ECC-521

La resposta correcta és: RSA-2048

Common Name (CN) de la entidad a la que se ha emitido el certificado: atenea.upc.edu ✔

10 primeros dígitos (base 10) del módulo si es una clave RSA, o de la componente x si es una clave ECC: 1961192334 ✖

```
-----BEGIN CERTIFICATE-----
MIIH0zCCBbugAwIBAgIRANePdG/REfbYeDEVGLl9BZ8wDQYJKoZIhvcNAQEMBQAw
RDELMAkGA1UEBhMCTkwxGTAXBgNVBAoTEEdFQU5UIFZlcmVuaWdpbmcxGjAYBgNV
BAMTEUdFQU5UIE9WIFJTQSBDQSA0MB4XDTIyMDIyMjAwMDAwMFoXDTIzMDIyMjIz
NTk1OVowajELMAkGA1UEBhMCRVMxEjAQBgNVBAgTCUJhcmNlbG9uYTEuMCwGA1UE
CgwlVW5pdmVyc2l0YXQgUG9saXTDqGNuaWNhIGRlIENhdGFsdW55YTEXMBUGA1UE
AxMOYXRlbmVhLnVwYy5lZHUwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIB
AQDEd+kxiYO8wg4Ncbhd23tX0+ikSyZlEdvzWpXunvo94n5lKzmxER2nEUnz7Xy3
yeeF0gzCXbB99tmVW+K8FadyPC1bNAjZUakvJ8k6+tgHQSKZRmxEXyy8lIzlz3zz
lIB+/2lYyY97bQLQuzfZQJshDCYxqeM9hOCx1u2WxS96+k5eKDeRZb4Q8VgqTtrr
4MCjILhtV+LDhaN1TMfhnS0p0E8flxN8eddlt+Ud6xLbf5h33QmEKgfq6LRV182+
/ob+4YSj1vsPmuHifNd0HNzBH9vhMNm76IA33M/XyzVG26frYCK+L1J+6hZvQCvz
ew1p9fqHMkBfvfRpQgjbE399AgMBAAGjggOYMIIDlDAfBgNVHSMEGDAWgBRvHTVJ
EGwy+lmgnryK6B+VvnF6DDAdBgNVHQ4EFgQUNH6IY5iwiclMweZ1voqLTaafiiAw
DgYDVR0PAQH/BAQDAgWgMAwGA1UdEwEB/wQCMAAwHQYDVR0lBBYwFAYIKwYBBQUH
AwEGCCsGAQUFBwMCMEkGA1UdIARCMEAwNAYLKwYBBAGyMQECAk8wJTAjBggrBgEF
BQcCARYXaHR0cHM6Ly9zZWN0aWdvLmNvbS9DUFMwCAYGZ4EMAQICMD8GA1UdHwQ4
MDYwNKAyoDCGLmh0dHA6Ly9HRUFOVC5jcmwuc2VjdGlnby5jb20vR0VBTlRPVlJT
QUNBNC5jcmwwdQYIKwYBBQUHAQEEaTBnMDoGCCsGAQUFBzAChi5odHRwOi8vR0VB
TlQuY3J0LnNlY3RpZ28uY29tL0dFQU5UT1ZSU0FDQTQuY3J0MCkGCCsGAQUFBzAB
hh1odHRwOi8vR0VBTlQub2NzcC5zZWN0aWdvLmNvbTCCAX4GCisGAQQB1nkCBAIE
ggFuBIIBagFoAHYArfe++nz/EMiLnT2cHj4YarRnKV3PsQwkyoWGNOvcgooAAAF/
IEMfswAABAMARzBFAiEA/+VVM4xSBaBvzT2OjT6vXwapKwsgAZkkCWw7SCdguIcC
IAqN/ixzcpUOqFTKRgaHbp2VK/+WYFGbZFHiMLrFzfsGAHYAejKMVNi3LbYg6jjg
Uh7phBZwMhOFTTvSK8E6V6NS61IAAAF/IEMfdwAABAMARzBFAiBb1mas/v3UFlT/
pfGthsFDAjhmtcPtZ3i7AtgbPm7VegIhALncmtH0z9UOXkQ3fO9OkDlsj622j9X1
lUB0+92MDRg8AHYA6D7Q2j71BjUy51covIlryQPTy9ERa+zraeF3fW0GvW4AAAF/
IEMfTgAABAMARzBFAiEAuke8SxDMdW8XkUWDXez2oEf3MSrXwEly+6xGNCpe0f4C
IB+JN2eFX2boHwTbCywYkePJzxvfCDrbT0xdQ6vb+pb1MIGPBgNVHREEgYcwgYSC
DmF0ZW5lYS51cGMuZWR1ghJhdGVuZWEtcGhkLnVwYy5lZHWCEmF0ZW5lYS10ZmUu
dXBjLmVkdYITYXRlbmVhbW9iaWwudXBjLmVkdYIOZWR1dGljLnVwYy5lZHWCEG0u
YXRlbmVhLnVwYy5lZHWCE21vb2RsZS5tb29jLnVwYy5lZHUwDQYJKoZIhvcNAQEM
BQADggIBAFUJZzHe6rNkOr2GFHpXkofkHnRp1rMoIgoTj8lQFWLqfVFU0oxOm/Tt
OcBuPeyHAFPiAj3FuQTs/aYsigajOPxK4Ix6WrMQl8b+tkVF95mvpKvRPWKetb/m
GozVd4hKfydGo7SUtTo/zsqGsC/fdswMXsrDacXZUjlvrws95KiJGScWz7bWySmL
ixEd0VLHp2ErBNWnFrcgBfI+FUBsEA7uZSHzzE0mlXKoks3niRxLs9oQ4v7PQf6H
aNtHPKInFFQqK7CrzmP+b7gezUOiWvz/Rye5O94b4raOLLpuar77ISrfuGNNUtmb
+Grl5uT0xjittyqyISqPRYO/S9x8eN6uhOVUkZpaOAtOmtMVOC/QKVMWrt041QDz
SJEEtRPquwUjSDpdOKpaNyRHS2JJK2aQjp9Dx2MhczVRHxCGvIeJUngteqbN8UTj
geeIX7sywCLBxC34gbnZjdoUafrF+g6jmVn9HddLeGETWuKdOJtOolzc4VJJASIK
SxT2L51D0k1Xrihm4TgLVyGE1ulwyOgq5gtQZ/XQ0IrNmCRMZD+PNDaKO9RCP5Q5
vO/ultpk4ionFj5MXEUar8D50T2GQ3lOkFx0YkLtk6hSYSnArmoQsFz1RKnfAtWc
aVQgcRdY7op36062caf3yc1eodCFe4qIHZJ6+MuKB+dGIHy5we/H
-----END CERTIFICATE-----
```