

Pregunta 1

Correcte

Puntuació 1,00 sobre 1,00

Marca la pregunta

Una CRL

Trieu-ne una o més:

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

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

Pregunta 2

Correcte

Puntuació 1,00 sobre 1,00

Marca la pregunta

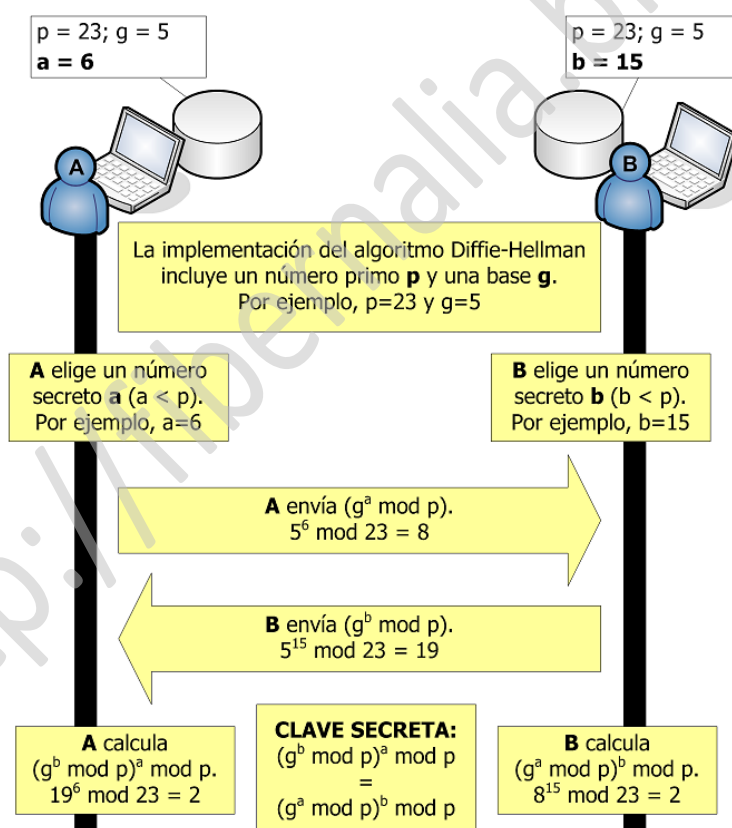
Dos usuarios desean acordar una clave secreta usando Diffie-Hellman con $p = 67$ y $g = 5$. El usuario A genera $a = 17$ y el B genera $b = 4$. La clave acordada es:

Trieu-ne una o més:

- ☐ a. 26
- ☒ b. 25 ✓
- ☐ c. 27

La resposta correcta és: 25.

Ejemplo de Diffie-Hellman



Projects

C

Files

New

Log

Find

Settings

Examen.sagews

Run

Stop

Restart

Help

in

out

Modes

Help

#

Data

Control

Program

x

Plots

Calculus

```

1
2 # Diffie-Hellman. p = 67, g = 5, a = 17, b = 4. Clave secreta?
3 p = 67
4 g = 5
5 a = 17
6 b = 4
7 alfa = mod((g^a),p)
8 alfa
9 beta = mod((g^b),p)
10 beta
11 deltaA = mod((beta^a),p)
12 deltaA
13 deltaB = mod((alfa^b),p)
14 deltaB
15
15      53
15      22
15      25
15      25

```

Pregunta 3

Correcte

Puntuació 1,00 sobre 1,00

Marca la pregunta

Una firma RSA

Triu-ne una o més:

- ☐ a. tiene el mismo tamaño que el hash del mensaje.
- ☐ b. tiene el mismo tamaño que el exponente de verificación de firma.
- ☒ c. tiene el mismo tamaño que el módulo. ✓

La resposta correcta és: tiene el mismo tamaño que el módulo..

Pregunta 4

Correcte

Puntuació 1,00 sobre 1,00

Marca la pregunta

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

Triu-ne una o més:

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

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

Pregunta 5

Correcte

Puntuació 1,00 sobre 1,00

Marca la pregunta

En el RSA, el exponente público se elige

Triu-ne una o més:

- ☒ a. preferentemente primo y de peso pequeño. ✓
- ☐ b. aleatoriamente.
- ☐ c. relativamente primo con p y q , ya calculados.

La resposta correcta és: preferentemente primo y de peso pequeño..

Pregunta 6

Correcte

Puntuació 1,00
sobre 1,00

▼ Marca la pregunta

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

Trieu-ne una o més:

- ☐ a. 1024 bits.
- ☒ b. 256 bits. ✓
- ☐ c. 512 bits.

La resposta correcta és: 256 bits..

Pregunta 7

Correcte

Puntuació 1,00
sobre 1,00

▼ Marca la pregunta

Una firma ECDSS

Trieu-ne una o més:

- ☐ a. triplica el tamaño del orden del generador.
- ☒ b. duplica el tamaño del orden del generador. ✓
- ☐ c. tiene el mismo tamaño que el orden del generador.

La resposta correcta és: duplica el tamaño del orden del generador..

Pregunta 8

Correcte

Puntuació 1,00
sobre 1,00

▼ Marca la pregunta

¿Cuál de las siguientes operaciones es más costosa?

Trieu-ne una o més:

- ☐ a. calcular inversos módulo p .
- ☒ b. Calcular potencias módulo p . ✓
- ☐ c. multiplicar módulo p .

La resposta correcta és: Calcular potencias módulo p ..

Pregunta 9

Correcte

Puntuació 1,00
sobre 1,00

▼ Marca la pregunta

Con ciertas implementaciones de RSA se puede l es el tamaño del módulo en bits):

Trieu-ne una o més:

- ☒ a. cifrar en $O(l^2)$ y firmar en $O(l^3)$. ✓
- ☐ b. firmar y verificar la firma en $O(l^2)$.
- ☐ c. cifrar y descifrar en $O(l^2)$.

La resposta correcta és: cifrar en $O(l^2)$ y firmar en $O(l^3)$..

Pregunta 10

Correcte

Puntuació 1,00
sobre 1,00

▼ Marca la pregunta

En el RSA

Trieu-ne una o més:

- ☒ a. se recomienda usar una clave para cifrar y otra diferente para firmar. ✓
- ☐ b. es indiferente usar una misma clave para cifrar y firmar que usar claves diferentes para cifrar y firmar.
- ☐ c. se recomienda usar la misma clave para cifrar y firmar.

La resposta correcta és: se recomienda usar una clave para cifrar y otra diferente para firmar..

Pregunta 11

Correcte

Puntuació 1,00
sobre 1,00

▼ Marca la pregunta

¿Para cuál de los sistemas de cifrado siguientes el criptograma es significativamente más largo que el mensaje?

Triu-ne una o més:

- ☒ a. ElGamal. ✓
- ☐ b. AES.
- ☐ c. RSA.

La resposta correcta és: ElGamal..

Pregunta 12

Incorrecte

Puntuació 0,00
sobre 1,00

▼ Marca la pregunta

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

Triu-ne una o més:

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

La resposta correcta és: Igual que en RSA..

Pregunta 13

Incorrecte

Puntuació 0,00
sobre 1,00

▼ Marca la pregunta

En una comunicació client-servidor usando TLS

Triu-ne una o més:

- ☐ a. el algoritmo de cifrado viene predefinido en las especificaciones del protocolo TLS.
- ☐ b. el algoritmo de cifrado lo elige el servidor entre los presentados por el cliente.
- ☒ c. el algoritmo de cifrado lo elige el cliente entre los presentados por el servidor. ✗

La resposta correcta és: el algoritmo de cifrado lo elige el servidor entre los presentados por el cliente..

Pregunta 14

Correcte

Puntuació 1,00
sobre 1,00

▼ Marca la pregunta

Si disposem de dos parells missatge-criptograma, (m_1, c_1) i (m_2, c_2) , xifrats amb un RSA amb la mateixa clau pública (n, e) , aleshores podem desxifrar

Triu-ne una o més:

- ☐ $c_1 + c_2$. El missatge corresponent és $m_1 + m_2$.
- ☐ Qualsevol criptograma que s'obtingui fent sumes i productes de c_1 i c_2 .
- ☒ $c_1 c_2$. El missatge corresponent és $m_1 m_2$. ✓

La teva resposta és correcta.

La resposta correcta és: $c_1 c_2$. El missatge corresponent és $m_1 m_2$..

Pregunta 15

Correcte

Puntuació 1,00
sobre 1,00

▼ Marca la pregunta

Un usuario tiene como clave RSA el par $(e, n) = (3, 451)$. Su exponente privado es:

Triu-ne una o més:

- ☐ a. 301
- ☐ b. 14
- ☒ c. 267 ✓

La resposta correcta és: 267.

```

1
2 # RSA. (e,n) = (3,451). Exponente privado?
3 e = 3
4 n = 451
5 factor(n)
6 p = 11
7 q = 41
8 fiDeN = (p-1)*(q-1)
9 d = inverse_mod(e,fiDeN)
10 d
11
11 11 * 41
    267

```

Pregunta 16

Correcte

Puntuació 1,00
sobre 1,00

Marca la pregunta

El test de Miller-Rabin se usa para buscar números

Tríeu-ne una o més:

- ☐ a. primos y tiene un coste $O(l^6)$, siendo l el tamaño en bits del número buscado.
- ☒ b. probablemente primos y tiene un coste $O(l^3)$, siendo l el tamaño en bits del número buscado. ✓
- ☐ c. aleatorios y tiene un coste $O(l^2)$, siendo l el tamaño en bits del número buscado.

La resposta correcta és: probablemente primos y tiene un coste $O(l^3)$ siendo l el tamaño en bits del número buscado..

Pregunta 17

Correcte

Puntuació 1,00
sobre 1,00

Marca la pregunta

Consideremos una curva elíptica E definida sobre \mathbb{Z}_p , $p=647$.

El número de puntos de la curva puede ser:

Tríeu-ne una o més:

- ☐ a. 589
- ☒ b. 686 ✓
- ☐ c. 310

La resposta correcta és: 686.

$$p + 1 - 2\sqrt{p} \leq |E(\mathbb{Z}_p)| \leq p + 1 + 2\sqrt{p}$$

$$647 + 1 - 2\sqrt{647} \leq 686 \leq 647 + 1 + 2\sqrt{647}$$

Pregunta 18

Correcte

Puntuació 1,00
sobre 1,00

Marca la pregunta

En un certificado digital

Trieu-ne una o més:

- ☒ a. figuren la clave pública del propietario y la firma digital de la Autoridad Certificadora. ✓
- ☐ b. figuren las claves pública y privada del propietario.
- ☐ c. figuren las claves públicas del propietario y de la Autoridad Certificadora.

La resposta correcta és: figuren la clave pública del propietario y la firma digital de la Autoridad Certificadora..

Pregunta 19

Correcte

Puntuació 1,00
sobre 1,00

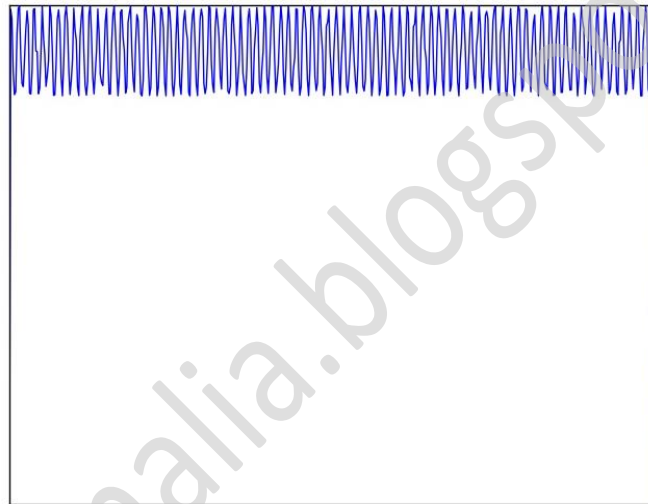
Marca la pregunta

Se ha calculado el hash de n entradas elegidas aleatoriamente y se ha dibujado el número de veces que el bit i -ésimo toma el valor 1.

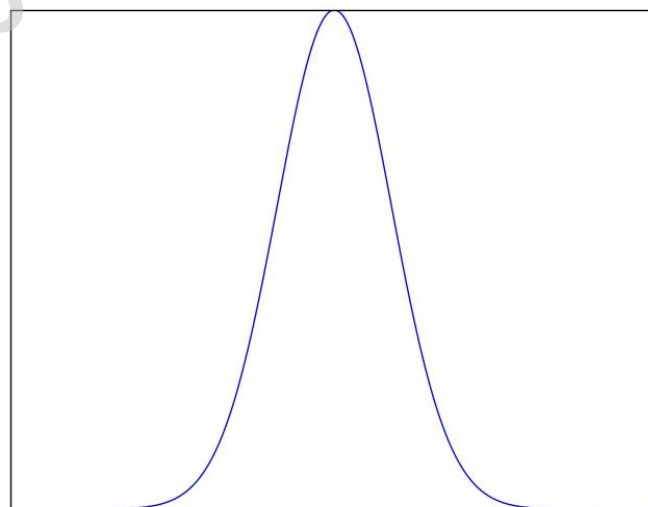
¿Qué gráfica hemos obtenido?

Trieu-ne una o més:

☒ a.



☐ b.



Pregunta 20

Correcte

Puntuació 1,00
sobre 1,00

Marca la pregunta

¿Qué longitud mínima de clave se recomienda en el RSA?

Trieu-ne una o més:

- ☒ a. 2048 bits ✓
- ☐ b. 1024 bits
- ☐ c. 4096 bits

La resposta correcta és: 2048 bits.

Pregunta 3

No s'ha respost
encara

Puntuat sobre 1,00

Marca la pregunta

Edita la pregunta OSCP

OCSP

Trieu-ne una:

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

Pregunta 7

No s'ha respost
encara

Puntuat sobre 1,00

Marca la pregunta

Edita la pregunta RSA:
Cálculo exponente
privado

Un usuario tiene como clave RSA el par $(e, n) = (3, 115)$. Su exponente privado es:

Trieu-ne una:

- ☒ a. 59
- ☐ b. 8
- ☐ c. 77

```
1
2 # RSA. (e,n) = (3,115). Exponente privado?
3 e = 3
4 n = 115
5 factor(n)
6 p = 5
7 q = 23
8 fiDeN = (p-1)*(q-1)
9 d = inverse_mod(e, fiDeN)
10 d
11
12 5 * 23
13 59
```


2. ¿Qué longitud mínima de clave se recomienda en ECDSA?

a) 512 bits.

b) 256 bits.

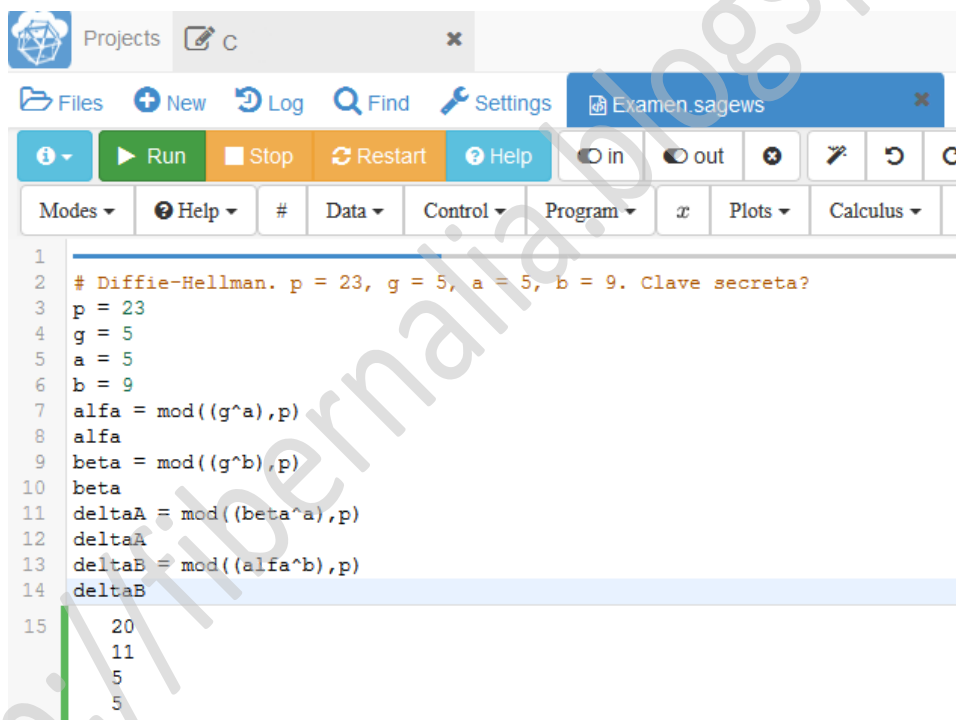
c) 1024 bits.

5. Dos usuarios desean acordar una clave secreta usando Diffie-Hellman con $p = 23$ y $g = 5$. El usuario A genera $a = 5$ y el B genera $b = 9$. La clave acordada es

a) 4

b) 2

c) 5



The screenshot shows a SageMath window titled 'Examen.sagews'. The code in the editor is as follows:

```
1
2 # Diffie-Hellman. p = 23, g = 5, a = 5, b = 9. Clave secreta?
3 p = 23
4 g = 5
5 a = 5
6 b = 9
7 alfa = mod((g^a),p)
8 alfa
9 beta = mod((g^b),p)
10 beta
11 deltaA = mod((beta^a),p)
12 deltaA
13 deltaB = mod((alfa^b),p)
14 deltaB
15
```

The output of the code is displayed on the right side of the window:

```
20
11
5
5
```

6. Un usuario tiene como clave RSA el par $(e, n) = (3, 33)$. Su exponente privado es

a) 7

b) 17

c) 27

The screenshot shows the SageMath web interface with a code editor and a command line. The code defines RSA parameters and calculates the private exponent d .

```

1
2 # RSA. (e,n) = (3,33). Exponente privado??
3 e = 3
4 n = 33
5 factor(n)
6 p = 3
7 q = 11
8 fiDeN = (p-1)*(q-1)
9 d = inverse_mod(e,fiDeN)
10 d
11
12 3 * 11
13 7

```

7. Con ciertas implementaciones de RSA se puede (l es el tamaño del módulo en bits):

- a) cifrar y descifrar un mensaje en $O(l^2)$.
- b) firmar y verificar la firma en $O(l^2)$.
- c) cifrar un mensaje y verificar una firma en $O(l^2)$.

8. Consideremos una curva elíptica E definida sobre \mathbb{Z}_{53} .

- a) La curva puede tener 41 puntos.
- b) La curva puede tener 79 puntos.
- c) La curva puede tener 31 puntos.

$$p + 1 - 2\sqrt{p} \leq |E(\mathbb{Z}_p)| \leq p + 1 + 2\sqrt{p}$$

$$53 + 1 - 2\sqrt{53} \leq 41 \leq 53 + 1 + 2\sqrt{53}$$

9. Sea $P = (5, 24)$ un punto de la curva elíptica E sobre \mathbb{Z}_{31} definida por $y^2 = x^3 - 3x + 1$ y que tiene 31 puntos. Hallar $30P$.

- a) Punto del infinito.
- b) $(5, 7)$
- c) $(5, 24)$

```

1
2 # P = (5,24), Z31, y2 = x3 - 3x + 1. Hallar 30P.
3 p = 31
4 a = -3
5 b = 1
6 Zp = Zmod(p)
7 E = EllipticCurve(Zp, [a,b])
8 P = E([5,24])
9 aux = 30*P
10 aux
11 (5 : 7 : 1)

```

12. El DNIe contiene

- a) dos certificados de ciudadano.
- b) únicamente un certificado de ciudadano.
- c) un único certificado de ciudadano y el certificado de la AC que lo emite.

Pregunta 13

No s'ha respost encara

Puntuat sobre 1,00

Marca la pregunta

Dos usuarios desean acordar una clave secreta usando Diffie-Hellman con $p = 31$ y $g = 5$.

El usuario A genera $a = 8$ y el B genera $b = 4$. La clave acordada es:

Trieu-ne una:

- ☒ a. 25
- ☐ b. 30
- ☐ c. 28

```

1
2 # Diffie-Hellman. p = 31, g = 5, a = 8, b = 4. Clave secreta?
3 p = 31
4 g = 5
5 a = 8
6 b = 4
7 alfa = mod((g^a),p)
8 alfa
9 beta = mod((g^b),p)
10 beta
11 deltaA = mod((beta^a),p)
12 deltaA
13 deltaB = mod((alfa^b),p)
14 deltaB
15 25
   5
  25
  25

```

Pregunta 14

No s'ha respost encara

Puntuat sobre 1,00

Marca la pregunta

Consideremos una curva elíptica E definida sobre \mathbb{Z}_p , $p=1021$.

El número de puntos de la curva puede ser:

Triu-ne una:

- ☒ a. 988
- ☐ b. 2233
- ☐ c. 1428

$$p + 1 - 2\sqrt{p} \leq |E(\mathbb{Z}_p)| \leq p + 1 + 2\sqrt{p}$$

$$1021 + 1 - 2\sqrt{1021} \leq 988 \leq 1021 + 1 + 2\sqrt{1021}$$

Pregunta 1

Correcte

Puntuació 1,00

sobre 1,00

Marca la pregunta

En el RSA, el exponente público se elige

Triu-ne una:

- ☐ a. relativamente primo con p y q , ya calculados.
- ☐ b. aleatoriamente.
- ☒ c. preferentemente primo y de peso pequeño. ✓

La respuesta correcta és: preferentemente primo y de peso pequeño.

Pregunta 2

Correcte

Puntuació 1,00

sobre 1,00

Marca la pregunta

Dos usuarios desean acordar una clave secreta usando Diffie-Hellman con $p=53$ y $g=3$. El usuario A genera $a=9$ y el B genera $b=6$. La clave acordada es:

Triu-ne una:

- ☒ a. 9 ✓
- ☐ b. 14
- ☐ c. 16

La respuesta correcta és: 9.

```
Projects C
Files New Log Find Settings Examen.sagews
Run Stop Restart Help in out
Modes Help # Data Control Program x Plots Calculus
1
2 # Diffie-Hellman. p = 53, g = 3, a = 9, b = 6. Clave secreta?
3 p = 53
4 g = 3
5 a = 9
6 b = 6
7 alfa = mod((g^a),p)
8 alfa
9 beta = mod((g^b),p)
10 beta
11 deltaA = mod((beta^a),p)
12 deltaA
13 deltaB = mod((alfa^b),p)
14 deltaB
15 20
40
9
9
```

Pregunta 3

Correcte

Puntuació 1,00
sobre 1,00

▼ Marca la pregunta

Una firma RSA

Trieu-ne una:

- ☐ a. tiene el mismo tamaño que el exponente de verificación de firma.
- ☒ b. tiene el mismo tamaño que el módulo. ✓
- ☐ c. tiene el mismo tamaño que el hash del mensaje.

La resposta correcta és: tiene el mismo tamaño que el módulo..

Pregunta 4

Correcte

Puntuació 1,00
sobre 1,00

▼ Marca la pregunta

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

Correcte

Puntuació 1,00
sobre 1,00

▼ Marca la pregunta

Con ciertas implementaciones de RSA se puede (l es el tamaño del módulo en bits):

Trieu-ne una:

- ☐ a. firmar y verificar la firma en $O(l^2)$.
- ☒ b. cifrar en $O(l^2)$ y firmar en $O(l^3)$. ✓
- ☐ c. cifrar y descifrar en $O(l^2)$.

La resposta correcta és: cifrar en $O(l^2)$ y firmar en $O(l^3)$.

Pregunta 6

Correcte

Puntuació 1,00
sobre 1,00

▼ Marca la pregunta

En el RSA

Trieu-ne una:

- ☐ a. se recomienda usar la misma clave para cifrar y firmar.
- ☒ b. se recomienda usar una clave para cifrar y otra diferente para firmar. ✓
- ☐ c. es indiferente usar una misma clave para cifrar y firmar que usar claves diferentes para cifrar y firmar.

La resposta correcta és: se recomienda usar una clave para cifrar y otra diferente para firmar..

Pregunta 7

Correcte

Puntuació 1,00
sobre 1,00

Marca la pregunta

En un certificado digital

Triu-ne una:

- ☐ a. figuren las claves públicas del propietario y de la Autoridad Certificadora.
- ☒ b. figuren la clave pública del propietario y la firma digital de la Autoridad Certificadora. ✓
- ☐ c. figuren las claves pública y privada del propietario.

La resposta correcta és: figuren la clave pública del propietario y la firma digital de la Autoridad Certificadora..

Pregunta 8

Correcte

Puntuació 1,00
sobre 1,00

Marca la pregunta

Consideremos una curva elíptica E definida sobre \mathbb{Z}_p , $p=1217$.

El número de puntos de la curva puede ser:

Triu-ne una:

- ☐ a. 2213
- ☐ b. 3266
- ☒ c. 1227 ✓

La resposta correcta és: 1227.

$$p + 1 - 2\sqrt{p} \leq |E(\mathbb{Z}_p)| \leq p + 1 + 2\sqrt{p}$$

$$1217 + 1 - 2\sqrt{1217} \leq 1227 \leq 1217 + 1 + 2\sqrt{1217}$$

Pregunta 9

Correcte

Puntuació 1,00
sobre 1,00

Marca la pregunta

Una firma ECDSA

Triu-ne una:

- ☒ a. duplica el tamaño del orden del generador. ✓
- ☐ b. triplica el tamaño del orden del generador.
- ☐ c. tiene el mismo tamaño que el orden del generador.

La resposta correcta és: duplica el tamaño del orden del generador..

Pregunta 10

Correcte

Puntuació 1,00
sobre 1,00

Marca la pregunta

¿Cuál de las siguientes operaciones es más costosa?

Triu-ne una:

- ☐ a. calcular inversos módulo p .
- ☒ b. Calcular potencias módulo p . ✓
- ☐ c. multiplicar módulo p .

La resposta correcta és: Calcular potencias módulo p .

Pregunta 11

Completada

Puntuación 1,50
sobre 5,00

✓ Marca la pregunta

Demuestra que si un usuario, que usa DSS o ECDSS, firma dos mensajes diferentes usando el mismo número aleatorio entonces es posible hallar, en un tiempo razonable, su clave de firma. Analiza el coste de recuperar la clave privada.

Comentari:

$$\text{Mensaje 1} \begin{cases} k \cdot G = (x_1, y_1) \\ r = x_1 \bmod n \\ s_1 = \frac{\text{SHA}(m_1) + d \cdot r}{k} \bmod n \end{cases} \quad \text{Mensaje 2} \begin{cases} k \cdot G = (x_1, y_1) \\ r = x_1 \bmod n \\ s_2 = \frac{\text{SHA}(m_2) + d \cdot r}{k} \bmod n \end{cases}$$

$k \in [2, n - 1]$ aleatorio

G punto generador

d clave privada que el atacante quiere hallar

La firma es el par (r,s)

$$s_1 - s_2 = \frac{\text{SHA}(m_1) - \text{SHA}(m_2) + dr - dr}{k} = \frac{\text{SHA}(m_1) - \text{SHA}(m_2)}{k}$$

$$k = \frac{\text{SHA}(m_1) - \text{SHA}(m_2)}{s_1 - s_2}$$

$$d = \frac{sk - \text{SHA}(m)}{r}$$

Pregunta 12

Correcta

Puntuación 1,00
sobre 1,00

✓ Marca la pregunta

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

Tríe-ne una:

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



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

Pregunta 13

Correcte

Puntuació 1,00
sobre 1,00

Marca la pregunta

En una comunicació client-servidor usando TLS

Trieu-ne una:

- ☐ a. el algoritmo de cifrado lo elige el cliente entre los presentados por el servidor.
- ☐ b. el algoritmo de cifrado viene predefinido en las especificaciones del protocolo TLS.
- ☒ c. el algoritmo de cifrado lo elige el servidor entre los presentados por el cliente. ✓

La resposta correcta és: el algoritmo de cifrado lo elige el servidor entre los presentados por el cliente..

Pregunta 14

Correcte

Puntuació 1,00
sobre 1,00

Marca la pregunta

¿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. La mitad que en RSA.
- ☒ b. Igual que en RSA. ✓
- ☐ c. El doble que en RSA.

La resposta correcta és: Igual que en RSA..

Pregunta 15

Correcte

Puntuació 1,00
sobre 1,00

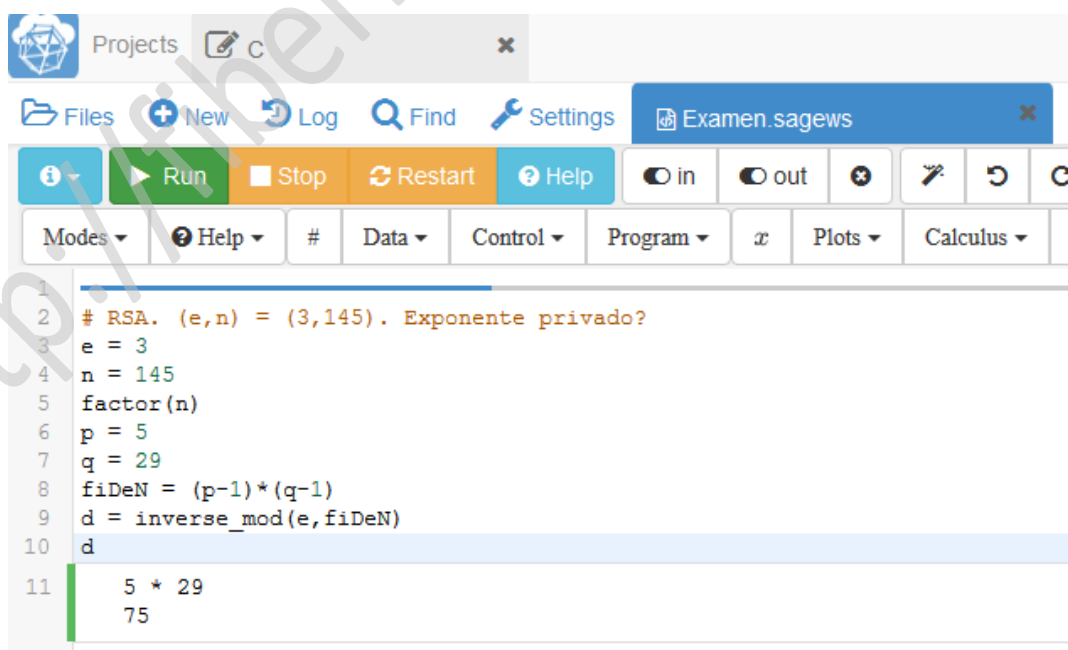
Marca la pregunta

Un usuario tiene como clave RSA el par $(e, n) = (3, 145)$. Su exponente privado es:

Trieu-ne una:

- ☐ a. 10
- ☒ b. 75 ✓
- ☐ c. 97

La resposta correcta és: 75.



```
1
2 # RSA. (e,n) = (3,145). Exponente privado?
3 e = 3
4 n = 145
5 factor(n)
6 p = 5
7 q = 29
8 fiDeN = (p-1)*(q-1)
9 d = inverse_mod(e, fiDeN)
10 d
11
12 5 * 29
13 75
```


Pregunta 16

Correcte

Puntuació 1,00
sobre 1,00

Marca la pregunta

El test de Miller-Rabin se usa para buscar números

Trieu-ne una:

- ☐ a. primos y tiene un coste $O(l^6)$, siendo l el tamaño en bits del número buscado.
- ☒ b. probablemente primos y tiene un coste $O(l^3)$, siendo l el tamaño en bits del número buscado.
- ☐ c. aleatorios y tiene un coste $O(l^2)$, siendo l el tamaño en bits del número buscado.

La resposta correcta és: probablement primos y tiene un coste $O(l^3)$, siendo l el tamaño en bits del número buscado.