Pregunta **8**

No s'ha respost encara

Puntuat sobre 1,0

¿Qué tamaño, en bytes, tendrá el criptograma correspondiente a un mensaje de 16011 bytes cifrado con el AES usando padding PKCS7?

Resposta:

Pregunta **9**

No s'ha respost encara

Puntuat sobre 1,0

Un usuario tiene como clave RSA el par $(e, n) = (3, 253)$. Su exponente privado es:

Trieu-ne una:

a. 147
b. 169
c. 8

Pregunta **10**

No s'ha respost encara

Puntuat sobre 1,0

Una CRL

Trieu-ne una:

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

Pregunta **11**

No s'ha respost encara

Puntuat sobre 1,0

Consideremos una curva elíptica $E$ definida sobre $\mathbb{Z}_p$, $p$=641.

El número de puntos de la curva puede ser:

Trieu-ne una:

- a. 1329
- b. 676
- c. 762

Pregunta **12**

No s'ha respost encara

Puntuat sobre 1,0

¿Cuál de las siguientes operaciones es más costosa?

Trieu-ne una:

- a. Calcular potencias módulo $p$.
- b. multiplicar módulo $p$.
- c. calcular inversos módulo $p$.