Pregunta **3**

No s'ha respost encara

Puntuat sobre 1,0

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

Trieu-ne una:

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

Pregunta **4**

No s'ha respost encara

Puntuat sobre 1,0

Si consideramos todas las subclaves de un AES-256, ¿cuántos bits tenemos?

Trieu-ne una:

- a. 1920
- b. 1408
- c. 1664

Pregunta **5**

No s'ha respost encara

Puntuat sobre 1,0

¿Qué longitud mínima de clave se recomienda en criptografía de clave secreta?

Trieu-ne una:

- a. 128 bits.
- b. 256 bits.
- c. 64 bits.

Pregunta **6**

No s'ha respost encara

Puntuat sobre 1,0

Un usuario cuya clave pública es un punto de la curva NIST P-521 ha firmado dos documentos usando el mismo número aleatorio. Los resultados son:

```
SHA512 del primer mensaje: 0x44c3b2b3325b2d409338901e92a50ac61fad749315f81550eb4

Primera firma: (4723700068028976880871463834135633162178027347601816257344538581
```

```
SHA512 del segundo mensaje: 0x9d9f403418d56aa5353754b0dad62b33b2ba7235134a2dfbbb

Segunda firma: (4723700068028976880871463834135633162178027347601816257344538581
```

Calcula su clave privada.

Resposta:

Pregunta **7**

No s'ha respost encara

Puntuat sobre 1,0

AES: Calcula el inverso de 0x33=x^5+x^4+x+1. (AES usa el polinomio irreducible $x^8+x^4+x^3+x+1$.)

Trieu-ne una:

- a. 0x07
- b. 0x6C
- c. 0x06