Començat el	dimecres, 19 d'octubre 2022, 09:02
Estat	Acabat
Completat el	dissabte, 22 d'octubre 2022, 09:41
Temps emprat	3 dies

Pregunta **1**

Completa

Puntuat sobre 1,0

Se ha cifrado un texto, en inglés, usando una permutación (Escítala)

Indica qué texto (identificado por los 10 primeros caracteres alfanuméricos del fichero descifrado) se corresponde con el texto cifrado TextoCifrado.txt

Resposta: RSSPQZEDLQ

La resposta correcta és: RSSPQZEDLQ

Pregunta **2**

Completa

Puntuat sobre 1,0

¿Cuál de los siguientes algoritmos de cifrado es incondicionalmente seguro?

Trieu-ne una:

- a. Cifrado de Vernam (One-Time Pad).
- b. Cifrado de César.
- c. Cifrado de Vigenère.

La resposta correcta és: Cifrado de Vernam (One-Time Pad).

Pregunta **3**

Completa

Puntuat sobre 1,0

AES: Calcula el inverso de 0x04=x^2. (AES usa el polinomio irreducible $x^8 + x^4 + x^3 + x + 1$.)

- a. 0xCB
- b. 0x2F
- c. 0x0C

La resposta correcta és: 0xCB

Pregunta **4**

Completa

Puntuat sobre 1,0

En el DES el número de rondas

Trieu-ne una:

- a. depende del tamaño del bloque.
- b. es fijo.
- c. depende del tamaño de la clave.

La resposta correcta és: es fijo.

Pregunta **5**

No s'ha respost

Puntuat sobre 1,0

Se ha cifrado un texto, en inglés, usando una sustitución monoalfabética (César)

Indica qué texto (identificado por los 10 primeros caracteres alfanuméricos del fichero descifrado) se corresponde con el texto cifrado TextoCifrado.txt

Resposta:

La resposta correcta és: RSSPQZEDLQ

Pregunta **6**

Completa

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.

La resposta correcta és: 128 bits.

Pregunta **7**

No s'ha respost

Puntuat sobre 1,0

Se ha cifrado un texto en inglés que sólo contiene letras mayúsculas (sin signos de puntuación, ni dígitos...) usando permutaciones y sustituciones polialfabéticas, en concreto $c = A \cdot m$, agrupando las letras de 3 en 3.

Indica qué texto (identificado por los 10 primeros caracteres alfanuméricos del fichero descifrado) se corresponde con el texto cifrado TextoCifrado.txt

Resposta:

Resposta:

La resposta correcta és: RSSPQZEDLQ

Pregunta **8**

Completa

Puntuat sobre 1,0

Considerad el cuerpo finito $GF(2^8)$ en el que se ha usado el polinomio irreducible $x^8 + x^5 + x^3 + x + 1$ para definir el producto.

El producto de los elementos a=85=0x55 y b=4=0x04 es:

Resposta: 127

La resposta correcta és: 127

◄ Test clave secreta

Salta a...

Why Cryptography Is Harder Than It Looks ►