Comenzado el	martes, 24 de enero de 2023, 12:59
Estado	Finalizado
Finalizado en	martes, 24 de enero de 2023, 12:59
Tiempo empleado	16 segundos

Pregunta **1**

Sin contestar

Puntúa como 1,0

AES: Calcula el inverso de 0x03=$x+1$. (AES usa el polinomio irreducible $x^8+x^4+x^3+x+1$.)

a. 0x56

b. 0x23

c. 0xF6

Pregunta **2**

Sin contestar

Puntúa como 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:

Respuesta:

Pregunta **3**

Sin contestar

Puntúa como 1,0

En el DES el número de rondas

Seleccione una:

a. es fijo.

b. depende del tamaño de la clave.

c. depende del tamaño del bloque.

Pregunta **4**

Sin contestar

Puntúa como 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

Respuesta:

Pregunta **5**

Sin contestar

Puntúa como 1,0

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

Seleccione una:

a. 128 bits.

b. 256 bits.

c. 64 bits.

Pregunta **6**

Sin contestar

Puntúa como 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

Respuesta:

Pregunta **7**

Sin contestar

Puntúa como 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

Respuesta:

Pregunta **8**

Sin contestar

Puntúa como 1,0

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

Seleccione una:

a. Cifrado de Vigenère.

b. Cifrado de Vernam (One-Time Pad).

c. Cifrado de César.

◄ Test clave secreta

Ir a...

Test clave pública ►