

## Pregunta 1

Correcte

Puntuació 1,00  
sobre 1,00

Marca la  
pregunta

En el AES, el resultado de aplicar *MixColumn* a un estado en el que todos los elementos son 0x8A es

Trieu-ne una o més:

- ☐ a. un estado en el que todos los elementos son 0x8A.
- ☐ b. un estado en el que todas las filas son diferentes pero las columnas son iguales.
- ☐ c. un estado en el que todas las filas son iguales pero las columnas son diferentes.

La resposta correcta és: un estado en el que todos los elementos son 0x8A..

```
public static void main(String[] args)
{
    word[] state = new word[4];
    for (int i = 0; i < 4; ++i)
    {
        word aux = new word();
        aux.byte1 = (byte) 0x8A;
        aux.byte2 = (byte) 0x8A;
        aux.byte3 = (byte) 0x8A;
        aux.byte4 = (byte) 0x8A;
        state[i] = aux;
    }
    printWords(mixColumns(state));
}
```

Output - Cryptography (run)

```
run:
8A 8A 8A 8A
8A 8A 8A 8A
8A 8A 8A 8A
8A 8A 8A 8A
BUILD SUCCESSFUL (total time: 0 seconds)
```

## Pregunta 2

Correcte

Puntuació 1,00  
sobre 1,00

Marca la  
pregunta

¿Cuál de las siguientes afirmaciones sobre el DES es cierta?

Trieu-ne una o més:

- ☐ a. Se ha roto mediante fuerza bruta.
- ☐ b. La clave y el bloque son de 56 bits.
- ☐ c. Todas las funciones que utiliza son lineales.

La resposta correcta és: Se ha roto mediante fuerza bruta..

1998 El 17 de julio la Electronic Frontier Foundation (EFF) presenta su DES craker que puede romper el DES utilizando la fuerza bruta en un tiempo medio de 4.5 días. Su coste: 220000\$.

## Pregunta 3

Correcte

Puntuació 1,00  
sobre 1,00

Marca la  
pregunta

En relación al cifrado de Vernam (One Time Pad), ¿cuál de las siguientes afirmaciones no es cierta?

Trieu-ne una o més:

- ☐ a. Satisface las condiciones de secreto perfecto de Shannon
- ☐ b. Es un estándar del NIST
- ☐ c. Usa un alfabeto de 32 caracteres, cada uno representado por 5 bits
- ☐ d. Las claves deben ser de un solo uso

La teva resposta és correcta.

La resposta correcta és: Es un estándar del NIST.

- Propuesto en 1917 para transmisiones telegráficas. Utiliza un alfabeto de 32 letras representadas por 5 bits.
- Su funcionamiento es igual que el criptosistema de Vigenère pero con una clave de longitud igual a la del mensaje.
- Las claves sólo se pueden utilizar una única vez.
- Es el único que es **incondicionalmente seguro**.

## SHANNON: SECRET PERFECTE



Claude Elwood Shannon (1916–2001)

### 1949: Communication Theory of Secrecy Systems

**Hipòtesi:** clau d'un sol ús i el criptoanalista només té accés al criptograma.

**Definició:** Un sistema criptogràfic és perfectament segur si el text clar és estadísticament independent del criptograma:

$$\text{Prob}(M = m / C = c) = \text{Prob}(M = m)$$

És a dir, la informació sobre el missatge aportada pel criptograma és nul·la. (Independentment del temps i recursos computacionals emprats)

## TEOREMES DE SHANNON

Basant-se en el concepte d'entropia, Shannon demostra:

- 1 És condició necessària que la longitud de la clau sigui més gran o igual que la del missatge
- 2 Existeixen sistemes perfectament segurs, en concret, el xifrat de Vernam ho és

- En el panorama criptogràfic actual el xifrat de Vernam és l'únic sistema incondicionalment segur que es coneix.
- És el sistema utilitzat en la **hotline** entre la Casa Blanca i el Kremlin que es va establir el 30 d'agost de 1963 i que es manté en funcionament.
- Les claus són transferides **a mà**, en presència de testimonis i en condicions de màxima seguretat

### Pregunta 4

Correcte

Puntuació 1,00  
sobre 1,00

Marca la pregunta

DES usa un algoritmo de expansión de clave para generar 16 subclaves, una para cada vuelta, de\_\_\_\_\_

Trieu-ne una o més:

- ☐ a. 64 bits
- ☐ b. 56 bits
- ☐ c. 48 bits
- ☐ d. 32 bits

La teva resposta és correcta.

La resposta correcta és: 48 bits.

**$k_1, k_2, \dots, k_{16}$  subclaus de 48 bits cadascuna**

► DES

### Pregunta 5

Correcte

Puntuació 1,00  
sobre 1,00

Marca la pregunta

Tenemos dos criptogramas correspondientes a dos mensajes diferentes cifrados con RC4 usando la misma clave. Además tenemos el mensaje correspondiente a uno de los criptogramas.

Trieu-ne una o més:

- ☐ a. Tenemos información suficiente para hallar fácilmente el otro mensaje.
- ☐ b. No tenemos información suficiente para hallar fácilmente ni la clave ni el otro mensaje.
- ☐ c. Tenemos información suficiente para hallar fácilmente la clave.

La respuesta correcta és: Tenemos información suficiente para hallar fácilmente el otro mensaje..

### Pregunta 6

Correcte

Puntuació 1,00  
sobre 1,00

Marca la pregunta

En el DES el número de rondas

Trieu-ne una o més:

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

La resposta correcta és: es fijo..

- 1 A un bloc  $X$  (64 bits), se li aplica una permutació inicial  $IP$ ,

$$x_0 = IP(X) \equiv L_0 R_0$$

- 2 Es realitzen 16 iteracions del tipus:

$$\begin{aligned} L_i &= R_{i-1}, \\ R_i &= L_{i-1} \oplus f(R_{i-1}, k_i), \end{aligned}$$

- 3 S'aplica la permutació inversa de  $IP$  a  $R_{16}L_{16}$ ,

$$Y = IP^{-1}(R_{16}L_{16})$$

### Pregunta 7

Correcte

Puntuació 1,00  
sobre 1,00

Marca la pregunta

¿Cuál de las siguientes afirmaciones sobre el RC4 es cierta?

Trieu-ne una o més:

- ☐ a. Es un cifrado de flujo.
- ☐ b. Es un cifrado modular.
- ☐ c. Es un cifrado de bloque.

La resposta correcta és: Es un cifrado de flujo..

- Algoritmo de cifrado de flujo desarrollado en 1987 por Ron Rivest para RSA Data Security.

### Pregunta 8

Correcte

Puntuació 1,00  
sobre 1,00

Marca la pregunta

En relación al Advanced Encryption Standard (AES), ¿cuál de estas afirmaciones no es cierta?

Trieu-ne una o més:

- ☐ a. Se basa en el algoritmo Rijndael
- ☐ b. Se desarrolló para substituir a DES
- ☐ c. Admite claves de 64, 128 y 256 bits
- ☐ d. Es un cifrado simétrico de bloque

La teva resposta és correcta.

La resposta correcta és: Admite claves de 64, 128 y 256 bits.

L'any 2001, l'algoritme **RIJNDAEL**, dissenyat per Joan Daemen (1965) i Vincent Rijmen (1970)



de la Universitat Catòlica de Leuven (Bèlgica), es converteix en el nou estàndard

Algoritme simètric de bloc de 128 bits i clau de 128, 192 o 256 bits. (AES-128, AES-192, AES-256)

2001 El DES es sustituido por el AES (Advanced encryption standard), aunque se mantiene el 3DES.

### Pregunta 9

Correcte

Puntuació 1,00  
sobre 1,00

▼ Marca la pregunta

¿Cuál de las siguientes afirmaciones sobre el AES es cierta?

Trieu-ne una o més:

- ☐ a. Es un cifrado de flujo.
- ☐ b. Es un cifrado modular.
- ☐ c. Es un cifrado de bloque.

La resposta correcta és: Es un cifrado de bloque..

### Pregunta 10

Correcte

Puntuació 1,00  
sobre 1,00

▼ Marca la pregunta

De los modos de operación

$$\text{ECB } (c_i = E_k(m_i)).$$

$$\text{CBC } (c_0 = IV, c_i = E_k(m_i \oplus c_{i-1})).$$

$$\text{CFB } (c_0 = IV, c_i = m_i \oplus E_k(c_{i-1})) \text{ y}$$

$$\text{OFB } (s_0 = IV, s_i = E_k(s_{i-1}), c_i = m_i \oplus s_i).$$

¿cuáles no requieren la inversa de  $E_k$  para descifrar?

Trieu-ne una o més:

- ☐ a. CBC y CFB.
- ☐ b. ECB y CBC.
- ☐ c. CFB y OFB.

La respuesta correcta és: CFB y OFB..

**Pregunta 11**

Correcte

Puntuació 1,00 sobre 1,00

Marca la pregunta

Si consideramos todas las subclaves de un AES-192, ¿cuántos bits tenemos?

Trieu-ne una:

- ☐ a. 1408
- ☐ b. 1920
- ☒ c. 1664 ✓

La resposta correcta és: 1664.

*The AES with a 128-bit key requires 11 subkeys of 128 bits → 1408 bits*

*The AES with a 192-bit key requires 13 subkeys of 128 bits → 1664 bits*

*The AES with a 256-bit key requires 15 subkeys of 128 bits → 1920 bits*

**Pregunta 12**

Correcte

Puntuació 1,00 sobre 1,00

Marca la pregunta

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

Trieu-ne una o més:

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

La resposta correcta és: 128 bits..

**Pregunta 13**

Correcte

Puntuació 1,00 sobre 1,00

Marca la pregunta

¿Cuál de las siguientes afirmaciones sobre el DES es cierta?

Trieu-ne una o més:

- ☐ a. Es un cifrado modular.
- ☐ b. Es un cifrado de bloque.
- ☐ c. Es un cifrado de flujo.

La resposta correcta és: Es un cifrado de bloque..

- Cifrado de bloques de 64 bits y clave de 56 bits.

**Pregunta 14**

Correcte

Puntuació 1,00 sobre 1,00

Marca la pregunta

El resultado de cifrar el mensaje *MI MAMA ME MIMA MUCHO* con la clave *LAVADAS* usando el cifrado de Vigenère es

Trieu-ne una o més:

- ☐ a. CX KMGV FD KZJH KQDZH
- ☐ b. XI HAPA EP MDMD MMNHJ
- ☐ c. SL FNXB GB HTIF XYYWS

La resposta correcta és: XI HAPA EP MDMD MMNHJ.



A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

- **Mensaje a cifrar:**

MI MAMA ME MIMA MUCHO (12 8 12 0 12 0 12 4 12 8 12 0 12 20 2 7 14)

- **Clave de cifrado:** LAVADAS (11 0 21 0 3 0 18)

- **Cifrado:** (si la suma da > 25, restar 26)

```

12 8 12 0 12 0 12 4 12 8 12 0 12 20 2 7 14
11 0 21 0 3 0 18 11 0 21 0 3 0 18 11 0 21

```

```

23 8 7 0 15 0 4 15 12 3 12 3 12 12 13 7 9

```

- **Criptograma:** XI HAPA EP MDMD MMNHJ

### Pregunta 15

Correcte

Puntuació 1,00  
sobre 1,00

Marca la pregunta

En el AES el número de rondas

Trieu-ne una o més:

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

La resposta correcta és: depende del tamaño de la clave..

- $N_k$  és el nombre de bits de la clau dividit per 32
- El nombre de voltes,  $N_r$ , depèn de la longitud de la clau:

$$N_k = \begin{cases} 128/32 = 4 \Rightarrow N_r = 10 \\ 192/32 = 6 \Rightarrow N_r = 12 \\ 256/32 = 8 \Rightarrow N_r = 14 \end{cases}$$

### Pregunta 16

Correcte

Puntuació 1,00  
sobre 1,00

Marca la pregunta

AES: Calcula el resultado de multiplicar  $0x02 = x$  y  $0xFC = x^7 + x^6 + x^5 + x^4 + x^3 + x^2$ . (AES usa el polinomio irreducible

$$x^8 + x^4 + x^3 + x + 1.)$$

Trieu-ne una o més:

- ☐ a. 0xD2
- ☐ b. 0xF4
- ☐ c. 0xE3

La resposta correcta és: 0xE3.

```
public static void main(String[] args)
{
    byte a = (byte) 0x02;
    byte b = (byte) 0xFC;
    byte c = GF_product_p(a,b);
    System.out.printf("%02X", c);
    System.out.println("");
}
```

```
Output - Cryptography (run)

run:
E3
BUILD SUCCESSFUL (total time: 0 seconds)
```

### Pregunta 17

Correcte

Puntuació 1,00  
sobre 1,00

Marca la pregunta

¿Qué tamaño tendrá el criptograma correspondiente a un mensaje de 16017 bytes cifrado con el AES en modo CBC?

Resposta:

16048



La resposta correcta és: 16048

Next 16-multiple of 16.017 + 16 = 16.032 + 16 = 16.048 bytes

### Pregunta 18

Correcte

Puntuació 1,00  
sobre 1,00

Marca la pregunta

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

Triu-ne una o més:

- ☐ a. 0x06  
☐ b. 0x07  
☐ c. 0x6C

La resposta correcta és: 0x6C.

```
public static void main(String[] args)
{
    GF_tables();
    byte a = (byte) 0x33;
    a = GF_invers(a);
    System.out.printf("%02X", a);
    System.out.println("");
}
```

```
Output - Cryptography (run)

run:
6C
BUILD SUCCESSFUL (total time: 0 seconds)
```

### Pregunta 19

Correcte

Puntuació 1,00  
sobre 1,00

Marca la pregunta

En el algoritmo DES (Data Encryption Standard), ¿cuántos bits son de clave y cuántos de paridad?

Trieu-ne una o més:

- ☐ a. 48 de clave y 16 de paridad
- ☐ b. 56 de clave y 8 de paridad
- ☐ c. 64 de clave y ninguno de paridad
- ☐ d. 48 de clave y 8 de paridad

La teva resposta és correcta.

La resposta correcta és: 56 de clave y 8 de paridad.

- Clau  $K$  de 56 bits (els bits 8,16,24,...,64 són bits de paritat)

### Pregunta 20

Correcte

Puntuació 1,00  
sobre 1,00

Marca la pregunta

¿Cuál de las siguientes afirmaciones sobre el AES es cierta?

Trieu-ne una o més:

- ☐ a. Todas las funciones que utiliza son lineales.
- ☐ b. Se ha roto mediante fuerza bruta.
- ☐ c. La clave puede ser de 128, 192 o 256 bits y el bloque es de 128 bits.

La resposta correcta és: La clave puede ser de 128, 192 o 256 bits y el bloque es de 128 bits..



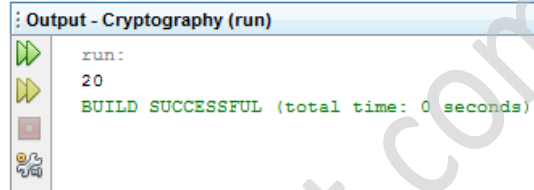
3. El AES usa el polinomio  $x^8 + x^4 + x^3 + x + 1$  para representar  $GF(2^8)$ . ¿Cuál es el inverso multiplicativo de  $0x3a = x^5 + x^4 + x^3 + x$ ?

a) 0x03

b) 0x02

c) 0x20

```
public static void main(String[] args)
{
    GF_tables();
    byte a = (byte) 0x3A;
    a = GF_invers(a);
    System.out.printf("%02X", a);
    System.out.println("");
}
```



```
run:
20
BUILD SUCCESSFUL (total time: 0 seconds)
```

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

a) Cifrado de César

b) Cifrado de Vigenère

c) Cifrado de Vernam (One-Time Pad)

9. El resultado de cifrar *MI MAMA ME MIMA* con el algoritmo de Vigenère con la clave *ALADA* es:

a) MT MDMA XE PIML

b) MT MAXA MP MIXA

c) OI EAOA EE OIEA

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

a) 1920

b) 3840

c) 2880

11. El resultado de aplicar *ByteSub* a 0x00 es

a) 0x63

b) 0x23

c) 0x0b

S-Box Values																
S(rs)	s															
	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
1	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
2	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
3	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
4	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
5	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
6	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
7	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
8	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
9	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
a	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
b	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
c	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
d	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
e	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
f	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

12. El resultado de aplicar *MixColumn* a un estado en el que todos los elementos son 0xFF es

- a) un estado en el que todos los elementos son 0xFF.
- b) un estado en el que todas las filas son iguales pero las columnas son diferentes.
- c) un estado en el que todas las filas son diferentes pero las columnas son iguales.

#### Pregunta 10

No s'ha respost encara

Puntuat sobre 1,00

Marca la pregunta

AES: Calcula el resultado de multiplicar  $0x02 = X$  y  $0x6C = X^6 + X^5 + X^3 + X^2$ . (AES usa el polinomio irreducible  $X^8 + X^4 + X^3 + X + 1$ .)

Tríeu-ne una:

- ☒ a. 0xD8
- ☐ b. 0xC7
- ☐ c. 0xE9

```
public static void main(String[] args)
{
    byte a = (byte) 0x02;
    byte b = (byte) 0x6C;
    byte c = GF_product_p(a,b);
    System.out.printf("%02X", c);
    System.out.println("");
}
```

Output - Cryptography (run)

```
run:
D8
BUILD SUCCESSFUL (total time: 0 seconds)
```

### Pregunta 1

Correcte

Puntuació 1,00  
sobre 1,00

▼ Marca la  
pregunta

Si consideramos todas las subclaves de un AES-128, ¿cuántos bits tenemos?

Trieu-ne una:

- ☐ a. 1920
- ☐ b. 1664
- ☒ c. 1408 ✓

La teva resposta és correcta.

La resposta correcta és: 1408

### Pregunta 2

Correcte

Puntuació 1,00  
sobre 1,00

▼ Marca la  
pregunta

¿Cuál de las siguientes afirmaciones sobre el DES es cierta?

Trieu-ne una:

- ☒ a. Se ha roto mediante fuerza bruta. ✓
- ☐ b. La clave y el bloque son de 56 bits.
- ☐ c. Todas las funciones que utiliza son lineales.

La respuesta correcta és: Se ha roto mediante fuerza bruta..

### Pregunta 3

Correcte

Puntuació 1,00  
sobre 1,00

▼ Marca la  
pregunta

¿Cuál de las siguientes afirmaciones sobre el AES es cierta?

Trieu-ne una:

- ☒ a. Es un cifrado de bloque. ✓
- ☐ b. Es un cifrado modular.
- ☐ c. Es un cifrado de flujo.

La respuesta correcta és: Es un cifrado de bloque..

### Pregunta 4

Correcte

Puntuació 1,00  
sobre 1,00

▼ Marca la  
pregunta

Tenemos dos criptogramas correspondientes a dos mensajes diferentes cifrados con RC4 usando la misma clave. Además tenemos el mensaje correspondiente a uno de los criptogramas.

Trieu-ne una:

- ☒ a. Tenemos información suficiente para hallar fácilmente el otro mensaje. ✓
- ☐ b. No tenemos información suficiente para hallar fácilmente ni la clave ni el otro mensaje.
- ☐ c. Tenemos información suficiente para hallar fácilmente la clave.

La respuesta correcta és: Tenemos información suficiente para hallar fácilmente el otro mensaje..

### Pregunta 5

Correcte

Puntuació 1,00  
sobre 1,00

▼ Marca la  
pregunta

En el AES, el resultado de aplicar *MixColumn* a un estado en el que todos los elementos son 0xF9 es

Trieu-ne una:

- ☐ a. un estado en el que todas las filas son diferentes pero las columnas son iguales.
- ☐ b. un estado en el que todas las filas son iguales pero las columnas son diferentes.
- ☒ c. un estado en el que todos los elementos son 0xF9. ✓

La respuesta correcta és: un estado en el que todos los elementos son 0xF9..

## Pregunta 6

Correcte

Puntuació 1,00  
sobre 1,00

Marca la pregunta

¿Cuál de las siguientes afirmaciones sobre el AES es cierta?

Trieu-ne una:

- ☒ a. La clave puede ser de 128, 192 o 256 bits y el bloque es de 128 bits. ✓
- ☐ b. Se ha roto mediante fuerza bruta.
- ☐ c. Todas las funciones que utiliza son lineales.

La resposta correcta és: La clave puede ser de 128, 192 o 256 bits y el bloque es de 128 bits..

## Pregunta 7

Correcte

Puntuació 1,00  
sobre 1,00

Marca la pregunta

¿Qué tamaño, en bytes, tendrá el criptograma correspondiente a un mensaje de 16052 bytes cifrado con el AES en modo CBC?

Resposta:

16080

16080

La resposta correcta és: 16080

Next 16-multiple of 16.052 + 16 = 16.064 + 16 = 16.080 bytes

## Pregunta 8

Correcte

Puntuació 1,00  
sobre 1,00

Marca la pregunta

El resultado de cifrar el mensaje *NO CENO EN CASA ESTA NOCHE* con la clave *PAGA* usando el cifrado de Vigenère es

Trieu-ne una:

- ☐ a. QD ZOVE ID BUYK LAFR PHUKL
- ☐ b. EI ETQC YY UWCX ZXXJ JGWFO
- ☒ c. CO IECO KN RAYA TSZA COIHT ✓

La resposta correcta és: CO IECO KN RAYA TSZA COIHT.

```
public static void main(String[] args)
{
    String text = "NO CENO EN CASA ESTA NOCHE";
    String key = "PAGA";
    String res = encrypt_vigenere(text, key);
    System.out.println(res);
}
```

Output - Cryptography (run)

```
run:
CO IECO KN RAYA TSZA COIHT
BUILD SUCCESSFUL (total time: 0 seconds)
```

### Pregunta 9

Correcte

Puntuació 1,00  
sobre 1,00

Marca la pregunta

De los modos de operación

ECB ( $c_i = E_k(m_i)$ ).

CBC ( $c_0 = IV$ ,  $c_i = E_k(m_i \oplus c_{i-1})$ ).

CFB ( $c_0 = IV$ ,  $c_i = m_i \oplus E_k(c_{i-1})$ ) y

OFB ( $s_0 = IV$ ,  $s_i = E_k(s_{i-1})$ ,  $c_i = m_i \oplus s_i$ ).

¿cuáles se pueden usar para asegurar la integridad de los mensajes?

Trieu-ne una:

- ☐ a. CFB y OFB.
- ☐ b. ECB y CBC.
- ☒ c. CBC y CFB. ✓

La resposta correcta és: CBC y CFB..

### Pregunta 10

Correcte

Puntuació 1,00  
sobre 1,00

Marca la pregunta

¿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 11

Correcte

Puntuació 1,00  
sobre 1,00

Marca la pregunta

AES: Calcula el resultado de multiplicar  $0x03 = X + 1$  y  $0x1A = X^4 + X^3 + X$ . (AES usa el polinomio irreducible  $x^8 + x^4 + x^3 + x + 1$ .)

Trieu-ne una:

- ☐ a. 0x3F
- ☒ b. 0x2E ✓
- ☐ c. 0x1D

La resposta correcta és: 0x2E.

```
public static void main(String[] args)
{
    byte a = (byte) 0x03;
    byte b = (byte) 0x1A;
    byte c = GF_product_p(a,b);
    System.out.printf("%02X", c);
    System.out.println("");
}
```

Output - Cryptography (run)

```
run:
2E
BUILD SUCCESSFUL (total time: 0 seconds)
```

## Pregunta 12

Correcte

Puntuació 1,00  
sobre 1,00

▼ Marca la pregunta

¿Cuál de las siguientes afirmaciones sobre el DES es cierta?

Trieu-ne una:

- ☐ a. Es un cifrado de flujo.
- ☐ b. Es un cifrado modular.
- ☒ c. Es un cifrado de bloque. ✓

La resposta correcta és: Es un cifrado de bloque..

## Pregunta 13

Correcte

Puntuació 1,00  
sobre 1,00

▼ Marca la pregunta

¿Cuál de las siguientes afirmaciones sobre el RC4 es cierta?

Trieu-ne una:

- ☒ a. Es un cifrado de flujo. ✓
- ☐ b. Es un cifrado modular.
- ☐ c. Es un cifrado de bloque.

La resposta correcta és: Es un cifrado de flujo..

## Pregunta 14

Correcte

Puntuació 1,00  
sobre 1,00

▼ Marca la pregunta

En relación al Advanced Encryption Standard (AES), ¿cuál de estas afirmaciones no es cierta?

Trieu-ne una:

- ☐ a. Se desarrolló para substituir a DES
- ☒ b. Admite claves de 64, 128 y 256 bits ✓
- ☐ c. Se basa en el algoritmo Rijndael
- ☐ d. Es un cifrado simétrico de bloque

La teva resposta és correcta.

La resposta correcta és: Admite claves de 64, 128 y 256 bits.

## Pregunta 15

Correcte

Puntuació 1,00  
sobre 1,00

▼ Marca la pregunta

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

Trieu-ne una:

- ☐ a. 0x0C
- ☒ b. 0xCB ✓
- ☐ c. 0x2F

La resposta correcta és: 0xCB.

```
public static void main(String[] args)
{
    GF_tables();
    byte a = (byte) 0x04;
    a = GF_invers(a);
    System.out.printf("%02X", a);
    System.out.println("");
}
```

Output - Cryptography (run)

```
run:
CB
BUILD SUCCESSFUL (total time: 0 seconds)
```



## Pregunta 16

Correcte

Puntuació 1,00  
sobre 1,00

Marca la pregunta

En relació al cifrado de Vernam (One Time Pad), ¿cuál de las siguientes afirmaciones no es cierta?

Triu-ne una:

- ☐ a. Las claves deben ser de un solo uso
- ☐ b. Satisface las condiciones de secreto perfecto de Shannon
- ☒ c. Es un estándar del NIST ✓
- ☐ d. Usa un alfabeto de 32 caracteres, cada uno representado por 5 bits

La teva resposta és correcta.

La resposta correcta és: Es un estándar del NIST.

<http://fibernalia.blogspot.com.es>