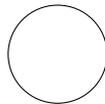


APELLIDOS: _____

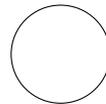
NOMBRE: _____

Selecciona las partes que vas a entregar

CRIPTOGRAFÍA



CÓDIGOS



1	2	3	4	5	CRIPTO
<input type="checkbox"/>	<input checked="" type="checkbox"/>				
10	10	10	10	12	52

A	B	C	D	CÓDIGOS
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
15	20	15	10	60

Os recuerdo que para aprobar la asignatura se ha de obtener una calificación de al menos un 5 en la parte de CÓDIGOS y una calificación de al menos un 5 en la parte de CRIPTOGRAFÍA

CRIPTOGRAFÍA

Razonar debidamente las respuestas

Si sólo entregas esta parte
tienes 1h 45 min

- **Incluir** todas las cuentas relativas al Algoritmo de Euclides/Teorema de Bezout y cuadrados iterados
 - **Factorización:** No se puede mediante fuerza bruta. Describe los algoritmos que utilices.
-

Vamos a utilizar el siguiente alfabeto

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

1. ¿Existe un cifrado afín sobre dígrafos (como elementos de $\mathbb{Z}/26^2\mathbb{Z}$) en el alfabeto anterior que envíe MADRID a BILBAO? En caso afirmativo, determinar donde va MALAGA

2. La clave pública RSA de Bruno es $(n, e) = (2599, 2085)$. A Bruno le han enviado el mensaje CDYADB. ¿Qué le han querido decir?

3. Sabemos que el número $n = 21449$ es producto de dos primos. Factoriza n usando el método de Kraitchik.

4. Usa el algoritmo Baby-step Giant-step para calcular $\log_2(-3)$ en $\mathbb{Z}/29\mathbb{Z}$.

5. Sea $n \in \mathbb{N}$ un número compuesto. Supongamos que n es pseudoprimo en base 2.

(a) ¿Es $2^n - 1$ compuesto?

(b) ¿Es $2^n - 1$ pseudoprimo en base 2?

TEORÍA DE CÓDIGOS

Razonar debidamente las respuestas

Si sólo entregas esta parte
tienes 1h 45 min

A. Sean los siguiente códigos

- Código 7-ario $C_1 = \{00000, 44202, 66303, 11404, 22101, 33505, 55606\}$.
- Código 6-ario $C_2 = \{201, 202, 231, 402, 403, 432, 003, 004, 033, 204, 205, 234, 405, 400, 435, 000, 001, 030, 404, 005, 200, 401, 002, 203, 433, 034, 235, 430, 031, 232, 035, 230, 431, 032, 233, 434\}$.
- Código ternario $C_3 = \{000, 201, 111, 021, 012, 120, 210\}$.

- (a) Determina cual de ellos es lineal.
 - (b) Determina los parámetros $(n, M, d)_q$ de cada uno de los códigos.
 - (c) Para aquellos que sean lineales además determina una matriz (de control) de paridad.
 - (d) En el caso en el que sea lineal muestra todos los elementos del código dual.
-

B. Hemos recibido una *información confidencial* que nos asegura que los números del próximo sorteo de la lotería primitiva son:

1152, 3123, 0220, 0550, 0004, 1461.

Pero como podréis ver, no es todo tan fácil. Resulta que nuestra *f fuente* nos ha mandado los 6 números de la combinación utilizando un código lineal sobre \mathbb{F}_7 que tiene la siguiente matriz generadora

$$G = \begin{pmatrix} 1 & 0 & 2 & 4 \\ 1 & 1 & 3 & 5 \end{pmatrix}.$$

Los números del 1 al 48 los ha puesto en base 7, es decir, el 1 es 01, el 2 es 02, así sucesivamente hasta el 48 que es 66 y el 49 que lo denota por 00. Así a un número $n = 7a + b$ con $a, b \in \mathbb{F}_7$ se le hace corresponder $(a, b)G \in \mathbb{F}_7^4$. Determinar la mayor cantidad de números de la *combinación ganadora*. Especifica en que condiciones tus números son los ganadores.

C. Denotamos por $A_q(n, d)$ el máximo M tal que existe un (n, M, d) -código q -ario. Calcular:

$$(i) A_q(n, 1) \quad (ii) A_q(n, n) \quad (iii) A_2(31, 3).$$

Para los apartados anteriores, dar un (n, M, d) -código q -ario con $M = A_q(n, d)$ para los respectivos parámetros.

D. Sea $C \subset \mathbb{F}_q^n$ un código lineal de dimensión k que corrige errores $e \in \mathbb{F}_q^n$ tales que $w(e) \leq t$. Demostrar $2t + k \leq n$.
