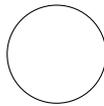


APELLIDOS: \_\_\_\_\_

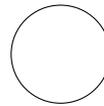
NOMBRE: \_\_\_\_\_

Selecciona las partes que vas a entregar

CRIPTOGRAFÍA



CÓDIGOS



1	2	3	4	<b>CRIPTO</b>
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
10	10	10	10	40

A	B	C	D	<b>CÓDIGOS</b>
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
10	10	10	10	40

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.

---

El alfabeto utilizado en los ejercicios 1 y 2 es el siguiente:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
P	Q	R	S	T	U	V	W	X	Y	Z	!	ı	ı	?
15	16	17	18	19	20	21	22	23	24	25	26	27	28	29

---

1. Hemos entrado en el ordenador central de la OTAN y hemos obtenido que cifran sus mensajes utilizando RSA y que su clave privada es  $(n, d) = (38009, 16123)$ . Enviar el mensaje **ASTANA** suplantando a la OTAN.

---

2. Recibimos el texto **CFPPCıMQBX** que ha sido encriptado mediante una función de cifrado matricial lineal sobre digrafos. Sabemos que el texto comienza por **EL PAIS**. Calcular la función de cifrado y descifrar el mensaje completo.

---

3. Sabemos que el número  $n = 2599$  es producto de dos primos. Factoriza  $n$  usando el método de Kraitchik. No vale por fuerza bruta.

---

4. 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  $C_3 = \{000, 201, 111, 021, 012, 120, 210\}$ .

- Determina cual de ellos es lineal.
  - Determina los parámetros  $(n, M, d)_q$  de cada uno de los códigos.
  - Para aquellos que sean lineales además determina una matriz (de control) de paridad.
- 

B. Calcula la matriz (de control) de paridad de un código Hamming  $\mathcal{H}_p(2)$  donde  $p$  es un número primo.

---

C. Se está utilizando un código lineal sobre  $\mathbb{F}_5$  que tiene la matriz generadora:

$$\mathcal{G} = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 2 \end{pmatrix}$$

y el 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

El número correspondiente a cada letra de la tabla anterior lo pasamos a base 5. Así todos los números de la tabla anterior se pueden escribir como  $x_0 + 5x_1$ . Esto es, como  $(x_0, x_1) \in \mathbb{F}_5^2$ . Ahora, cada letra del alfabeto la codificamos mediante  $(x_0, x_1)\mathcal{G} = (y_0, y_1, z_0, z_1) \in \mathbb{F}_5^4$ , obteniendo una pareja de letras correspondiente a la pareja de números  $(y_0 + 5y_1, z_0 + 5z_1)$ .

- Codificar la palabra **CASA**.
  - Recibimos el mensaje **VPCC**. Asegúrate qué nos han querido decir usando decodificación por mínima distancia.
- 

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  $2t + k \leq n$ .

---