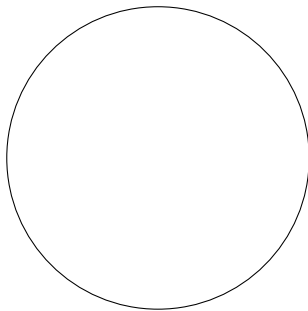


APELLIDOS: _____

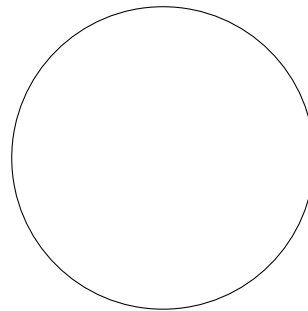
NOMBRE: _____

Firma en las partes que vas a entregar

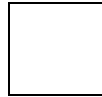
CRIPTOGRAFÍA



CÓDIGOS

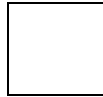


1



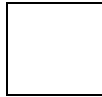
15

2



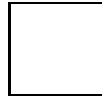
15

4



15

5



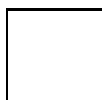
15

CRIPTO



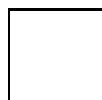
60

A



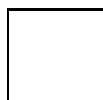
10

B



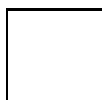
10

C



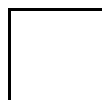
10

D



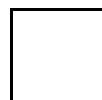
10

E



10

F



10

CÓDIGOS



60

Os recuerdo que para aprobar la asignatura se ha de obtener una calificación de al menos un 30 en la parte de **CÓDIGOS** y una calificación de al menos un 30 en la parte de **CRIPTOGRAFÍA**

CRIPTOGRAFÍA

Razonar debidamente las respuestas

- **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. Somos una organización que está espionando la correspondencia de Álvaro Ortiz, uno de los CEO de NVIDIA en España. Hemos interceptado el mensaje

TXAJMOMFOP

Sabemos que NVIDIA siempre utiliza un cifrado matricial afín sobre digrafos para transmitir sus mensajes y que una de las normas de la compañía es firmar todos los mensajes con el nombre del remitente. Descifra el mensaje.

-
2. La clave pública RSA de Maeva es $(n, e) = (106499, 57731)$. A Maeva le han enviado el mensaje DVFT. ¿Qué le han querido decir?

-
3. Sea $\mathbb{F}_{27} = \mathbb{F}_3(\alpha)$ donde $\alpha^3 + 2\alpha + 2 = 0$. Calcular $\log_\alpha(2\alpha^2 + 2)$.

-
4. Sea $n \in \mathbb{N}$ un entero impar compuesto y sea

$$L_n = \{ a \in (\mathbb{Z}/n\mathbb{Z})^\times : a^{n-1} \equiv 1 \pmod{n} \}.$$

Decide si la siguiente afirmación es verdadera o falsa:

- Si $|L_n| > \frac{1}{2}\varphi(n)$ entonces n es un número de Carmichael.

$$(67070 + k)^m \pmod{106499}$$

$m \backslash k$	1	2	3	4	5	6	7	8	9	10
1	67071	67072	67073	67074	67075	67076	67077	67078	67079	67080
2	1281	28925	56571	84219	5370	33022	60676	88332	9491	37151
3	79757	71816	40311	91747	13132	17470	104767	62031	102266	12480
4	43476	105980	89590	6561	82170	9223	13045	105987	87426	76260
5	36176	14805	76993	18646	16502	95756	23681	55241	81219	54333
6	100278	4284	14979	44047	27543	81265	17852	36091	26457	48862
7	14391	2146	81400	19719	8572	99322	90347	83329	9767	49736
8	18324	56363	70965	21125	85298	77527	93122	49146	85244	103206
9	10544	90632	75638	75554	24072	67880	71545	45342	44467	90985
10	43264	13083	81210	60580	104560	73632	72526	52234	84400	29108
11	87990	57715	476	86573	83353	48907	58681	41651	87259	11974
12	41704	34828	83547	45926	24472	103734	48896	77511	61421	462
13	39248	34550	90048	63448	96812	56118	53788	1678	38945	106250
14	66825	25859	18216	11112	101373	70312	71053	93940	77684	17423
15	9160	78633	45240	46286	58821	45996	85332	80987	75465	14814
16	84128	29098	13012	34815	56621	58165	25809	38495	6267	87450
17	19070	66881	101070	84236	99235	97673	49048	99355	32540	74581
18	97479	104552	87263	60516	125	15165	25588	40268	53655	102955
19	40399	85089	19157	53797	77453	35591	28392	69266	96539	80747
20	53771	20996	7026	87359	32256	20332	35066	99374	67886	76119
21	99104	7435	103322	49085	44015	69537	91667	36762	40752	74464
22	82297	52002	13578	17204	47346	33608	27594	43590	93575	29022
23	5416	35894	44245	24431	39269	25875	76617	106474	79363	100539
24	94946	72473	50250	91280	34907	83796	22765	27034	25164	446
25	15461	81698	44397	100208	6510	2773	25243	28179	73305	97960
26	3968	61708	21442	93003	12350	54494	103609	46710	60766	62001
27	103226	8339	16770	10796	27028	87365	82149	12800	86287	28132
28	77555	87159	78271	44203	77122	93764	50213	3462	38021	38779
29	67247	91839	2578	46361	88722	15619	27	56216	79106	57245
30	90887	29747	66317	59912	77028	29381	596	46755	38699	66656
31	92215	38518	42907	10721	67113	102460	40767	49338	83595	30464
32	22840	26554	85233	19106	104743	13492	59735	37939	83657	22308
33	20024	47111	73188	13377	4194	67389	32718	78637	89094	3191
34	77314	3662	80317	101322	48691	47507	393	23715	38542	95789
35	90984	30970	63224	51141	50491	22953	56008	85706	95593	15454
36	101663	63344	46170	5143	15625	45884	96391	64549	84556	99553
37	40598	44161	88987	11321	96715	583	64817	100977	8182	101944
38	88525	16404	101594	6884	91537	20175	14733	105305	51031	102730
39	34526	7919	88845	64251	70426	82006	41220	102615	17591	4106
40	85589	32655	55639	89539	60805	67605	93401	72101	84268	24066
41	30721	84225	43188	47278	9671	52059	42204	58290	72248	35438
42	52038	6244	82423	10348	103415	20272	67789	78833	86597	16861
43	55470	43500	101288	27769	68257	91939	1449	71626	65206	16500
44	98803	91895	12315	16895	52764	75769	67485	39441	39344	82392
45	22237	58314	104250	65870	77031	42665	57849	81739	4457	89755
46	45831	60833	61906	53365	55340	62911	46308	625	28410	57433
47	50364	1288	38126	79119	14354	8359	51882	69643	21284	4315
48	28562	18047	77709	89135	43590	77548	21091	41018	90341	92417
49	84389	87249	8198	128	82203	91989	94790	3739	84340	25570
50	58765	57876	10117	65552	99997	21601	25532	105996	2982	69205

TEORÍA DE CÓDIGOS

Razonar debidamente las respuestas

Si sólo entregas esta parte
tienes 1h 45 min

A. Decide si es cierta o falsa la siguiente afirmación:

- Sea $\mathbb{F}_q$ un cuerpo finito. El conjunto $C = \{(a+b, a, b) : a, b \in \mathbb{F}_q\} \subset \mathbb{F}_q^3$ es un $(3, q^2, 2)_q$ -código.

B. Sean $x = (x_1, \dots, x_n)$ e $y = (y_1, \dots, y_n)$ elementos de $\mathbb{F}_p^n$ y $z = (x_1y_1, \dots, x_ny_n)$. Decidir si la igualdad

$$d_H(x, y) = w(x) + w(y) - 2w(z)$$

es cierta para

- (a) $p = 2$, (b) $p = 3$, (c) $p \neq 2, 3$ primo.

C. Se me ha olvidado mi número PIN para poder pagar con mi tarjeta de crédito. Mi banco me informa como recuperarlo. El código PIN utiliza sólo los números 0, 1, 2, 3, 4 y consta de 4 cifras. Una vez creado se almacena una 6-tupla de la siguiente forma: para $(x_1, x_2, x_3, x_4) \in \mathbb{F}_5^4$ se almacena $(x_1, x_2, x_3, x_4)G = (y_1, y_2, y_3, y_4, y_5, y_6) \in \mathbb{F}_5^6$ donde

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

Nuestro banco nos manda la codificación de nuestro PIN. Lo que recibimos es 105144. Determina mi PIN. Demuestra en que condiciones es correcta la respuesta que das.

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

E. Sea $\mathbb{F}_4 = \mathbb{F}_2(\alpha)$ tal que $\alpha^2 + \alpha + 1 = 0$ y $C \subset \mathbb{F}_4^6$ con matriz generadora

$$G = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & \alpha & \alpha^2 \\ 0 & 0 & 1 & 1 & \alpha^2 & \alpha \end{pmatrix}.$$

Determinar $d(C)$.

F. Sea $C \subseteq \mathbb{F}_q^n$ un código lineal y sea $C^\perp$ su código dual. Decide si las siguientes afirmaciones son ciertas.

- (a) Si $d(C^\perp) = 2$ entonces no existe $c \in C$ tal que $w(c) \leq 2$.
(b) Si $d(C^\perp) \geq 3$ entonces no existe $c \in C$ tal que $w(c) \leq 2$.
-