TEORÍA DE CÓDIGOS Y CRIPTOGRAFÍA

Examen Final 27-01-2011

APELLIDOS, NOMBRE: _____

Ejercicio 1	Ejercicio 2	Ejercicio 3	Ejercicio 4	Ejercicio 5	FINAL
2 puntos	3 puntos	1 punto	3 puntos	1 punto	10

El alfabeto utilizado es el siguiente:

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

1. Recibimos un mensaje cifrado que sabemos comienza ZQCNGNRZOCVG y termina FGRZGO. Hemos averiguado que han utilizado un cifrado matricial afín sobre vectores de $(\mathbb{Z}/26\mathbb{Z})^2$. Más aún, el texto comienza con el título de una famosa canción y termina con el autor. Pero aún hemos conseguido más información: el autor de la canción es SERRAT. ¿Cuál es el título de la canción? Calcular la transformación afín de cifrado (matriz y vector).

2. Mi clave pública RSA es $(n, e) = (9797, 1477)$. Alguien ha utilizado esta clave pública para mandarme el siguiente mensaje:

NIWJRJHXAIBNNDC

Pero como soy muy despistado, no encuentro donde guardé mi clave secreta para poder descifrar el mensaje. Calcula mi clave secreta y descifra el mensaje.

3. Sea C el código binario formado por las palabras $00000, 10110, 01011$ y 11101.

(i) Calcular los parámetros n, M y d del código.

(ii) ¿Es lineal? En caso afirmativo, calcular las matrices generadoras de C y su dual.

(iii) ¿Es perfecto?

(iv) Si recibimos la palabra $r = 00011$. Decodificar r.

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

$$1152, \quad 3123, \quad 0220, \quad 0550, \quad 0004, \quad 1461.$$

Pero como podréis ver, no es todo tan fácil. Resulta que nuestra *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*.

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

$$(i)\ A_q(n, 1) \qquad (ii)\ A_q(n, n) \qquad (iii)\ A_2(15, 3).$$

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

No se pueden usar apuntes, libros u otros materiales, excepto calculadora no científica.
Razonar las respuestas. Aquellas soluciones que no sean justificadas no serán dadas como válidas.