TEORÍA DE CÓDIGOS Y CRIPTOGRAFÍA

Examen Extra. : 27-6-2012

APELLIDOS, NOMBRE: _____

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

• La nota FINAL se obtiene como la suma de los 5 ejercicios y dividiéndolo por 2. Para aprobar es **NECESARIO** sacar un mínimo de 3 puntos entre los ejercicios **1** y **2** y otros 3 puntos entre los ejercicios **3**, **4** y **5**.

• **Razonar debídamente las respuestas**

• **Incluir** todas las cuentas relativas al Algoritmo de Euclides/Teorema de Bezout y cuadrados iterados

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	!	¡	¿	?
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 **CFPPC¿MQBX** 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. Calcular $A_{11}(10, 3)$.

4. Un código lineal C se dice autodual si $C = C^{\perp}$. Demostrar

(i) C es un $[2m, m]$-código para algún entero positivo m.

(ii) Toda matriz generadora de C es matriz de paridad y recíprocamente.

(iii) Si $G = (Id_m|A)$ es una matriz generadora de C, entonces $H = (-A^{\top}|Id_m)$ también lo es.

5. Sea C el código lineal generado por la matriz

$$G = \begin{pmatrix} 0 & 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 2 & 0 & 1 & 0 \\ 0 & 0 & 3 & 0 & 1 & 1 \\ 0 & 1 & 4 & 0 & 1 & 0 \end{pmatrix} \in M_{4x6}(\mathbb{F}_5).$$

(i) Demostrar que es un código Hamming $Ham(r, q)$ y determinar r y q.
(ii) Se ha utilizado el código C para cifrar digrafos escritos en el alfabeto de 25 letras en el que $A = 0$, $B = 1, \ldots, Z = 24$ de la siguiente forma: cada digrafo corresponde a un par $(n, m) \in (\mathbb{Z}/25\mathbb{Z})^2$. Escribimos $n = 5a + b$ y $m = 5c + d$ con $a, b, c, d \in \mathbb{F}_5$. Así cada digrafo corresponde a un vector $(a, b, c, d) \in (\mathbb{F}_5)^4$ y lo codificamos mediante $(a, b, c, d) \cdot G \in (\mathbb{F}_5)^6 = (x_1, x_2, x_3, x_4, x_5, x_6)$. Así convertimos el digrafo definido por el par $(5a + b, 5c + d)$ en el trigrafo que viene dado por $(5x_1 + x_2, 5x_3 + x_4, 5x_5 + x_6)$. Si recibimos el mensaje **FSPUSP**. Asegúrate que hemos recibido o que hemos de hacer.