TEORÍA DE CÓDIGOS Y CRIPTOGRAFÍA

Examen Final : 25-1-2012

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 el 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. Creamos el siguiente criptosistema: a cada digrafo escrito en nuestro alfabeto le corresponde un vector $(x, y) \in (\mathbb{Z}/30\mathbb{Z})^2$. Ahora aplicamos la función g_1 y luego al resultado obtenido le aplicamos la función g_2, donde $g_1, g_2 : (\mathbb{Z}/30\mathbb{Z})^2 \to (\mathbb{Z}/30\mathbb{Z})^2$ están definidas por

$$g_1(x,y) = \begin{pmatrix} 3 & 1 \\ 17 & 2 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} + \begin{pmatrix} 2 \\ 3 \end{pmatrix} \quad ; \quad g_2(u,v) = \begin{pmatrix} 1 & 1 \\ 19 & 2 \end{pmatrix} \begin{pmatrix} u \\ v \end{pmatrix}.$$

Descifrar el mensaje cifrado **B¿VEMF**.

2. Bruno ha recibido el mensaje **GTAF?**. Descifrarlo sabiendo que su clave pública RSA es $(n, e) = (8388607, 5864343)$.

3. Para cada uno de los siguientes códigos calcular los parámetros $(n, M, d)_q$ y en el caso en el que sea lineal dar una matriz generadora y describir su código dual.

$$C_1 = \{00, 01, 02, 10, 20, 11, 22, 21, 12\} \subseteq (\mathbb{Z}/3\mathbb{Z})^2 \qquad C_2 = \{00, 10, 01, 11\} \subseteq (\mathbb{Z}/7\mathbb{Z})^2$$
$$C_3 = \{00000, 11111, 22222, 33333, 44444, 55555, 66666, 77777, 88888, 99999\} \subseteq (\mathbb{Z}/10\mathbb{Z})^5$$

4. Dar un ejemplo de un código con parámetros $[11, 9, 3]_{23}$ o en su caso demostrar su no existencia.

5. Vamos a utilizar el código lineal binario generado por la matriz

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

para transmitir el movimiento que ha de realizar un robot que hemos mandado a Marte. Para ello transcribimos las ocho puntos cardinales como

N	NE	E	SE	S	SO	O	NO
0	1	2	3	4	5	6	7

El número correspondiente a cada letra de la tabla anterior lo pasamos a base 2. Así todos los números de la tabla anterior se pueden escribir como $x_2 \cdot 4 + x_1 \cdot 2 + x_0$. Esto es, como $(x_2, x_1, x_0) \in \mathbb{F}_2^3$. Ahora, cada unos de los 8 puntos cardinales los codificamos mediante $(x_2, x_1, x_0)G \in \mathbb{F}_2^6$. En cada una de las siguientes transmisiones decidir que debe de hacer el robot y porque:

111110	001000	000001