TEORÍA DE CÓDIGOS Y CRIPTOGRAFÍA

Examen 8-9-2011

APELLIDOS, NOMBRE: _____

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

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.

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	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. Queremos utilizar digrafos como unidades de mensaje sobre el alfabeto habitual de 26 letras (sin Ñ). Para ello vamos a considerar dos criptosistemas. Uno de ellos considerando los digrafos como vectores de $(\mathbb{Z}/26\mathbb{Z})^2$ y cifrado matricial afín: $f : (\mathbb{Z}/26\mathbb{Z})^2 \longrightarrow (\mathbb{Z}/26\mathbb{Z})^2$. El otro considerando los digrafos como elementos de $\mathbb{Z}/26^2\mathbb{Z}$ y cifrado afín: $g : \mathbb{Z}/26^2\mathbb{Z} \longrightarrow \mathbb{Z}/26^2\mathbb{Z}$. Determinar f y g (si existen) de tal forma que envíen `MADRID` a `BILBAO`.

2. He enviado la misma palabra a tres amigos cifrándola mediante RSA. Las claves públicas de mis tres amigos son: $(n_1, e) = (33689197, 3)$, $(n_2, e) = (48746413, 3)$ y $(n_3, e) = (56010247, 3)$. He utilizado el alfabeto habitual de 26 letras (sin Ñ). Los mensajes cifrados que les ha llegado a cada uno de ellos, respectivamente, son: $c_1 =$`EEWNRB`, $c_2 =$`MEEPKA` y $c_3 =$`NGQGNE`. ¿Qué palabra les he enviado?

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

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

(a) Calcular los parámetros del código generado por $\mathcal{G}$ y determinar cuantos errores puede corregir.
(b) Se utiliza la correspondencia decimal de la tabla de caracteres ASCII para las letras (mayúsculas y minúsculas) del alfabeto como aparece en las siguientes tablas:

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
65	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80	81	82	83	84	85	86	87	88	89	90

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
97	98	99	100	101	102	103	104	105	106	107	108	109	110	111	112	113	114	115	116	117	118	119	120	121	122

El número decimal correspondiente a cada letra de la tabla anterior lo pasamos a base 5. Así todos los números decimales de las tablas anteriores se pueden escribir como $x_1 + x_2 5 + x_3 5^2$. Esto es, como $(x_1, x_2, x_3) \in \mathbb{F}_5^3$.
Ahora, cada letra (mayúscula o minúscula) del alfabeto la codificamos mediante $(x_1, x_2, x_3)\mathcal{G} \in \mathbb{F}_5^6$.
Si recibimos el mensaje `NIdW`. ¿Qué palabra nos han enviado?

4. Denotamos por $A_q(n, d)$ el máximo M tal que existe un $(n, M, d)_q$-código.
(a) Calcular $A_{11}(12, 3)$.
(b) Describir las palabras código de un $(12, M, 3)_{11}$-código con $M = A_{11}(12, 3)$.