Teoría de Códigos y Criptografía

Curso 2009-2010 3 de Febrero de 2010

Apellidos y Nombre _____

D.N.I. _____

El examen dura tres horas. No se pueden usar apuntes, libros u otros materiales. Se puede usar calculadoras. Todas las soluciones tienen que estar justificadas (no vale dar sólo las respuestas finales).

1. (2 puntos) Encuentra la transformación afín sobre vectores de $(\mathbb{Z}_{26})^2$, donde $0, ..., 25$ equivalen a las letras $A, ..., Z$ del alfabeto ingles, que transforma MUNICH a LONDON. (Notar que la transformación actúa sobre digrafos)

2. a) (1,5 puntos) Encontrar todas las soluciones de la siguiente congruencia:

$$x^2 \equiv 210 \pmod{9991}.$$

   b) (0,5 punto) Sean p y q dos números primos distintos impares. ¿Cuántas soluciones tiene la congruencia

$$x^2 \equiv 1 \pmod{pq}?$$

3. a) (1 punto) Factoriza el número 7519.

   b) (1 punto) Encuentra la clave privada de un usuario de un criptosistema basado en el RSA si su clave pública es $(7519, 49)$.

4. (1 punto) Sean N un número natural y $a, b \leq N$. Explica como calcular $a^b \pmod{N}$ de forma eficiente y da una cota superior que depende de N para el número de bit-operaciones necesarias para hacerlo.

5. Consideramos el código lineal sobre $\mathbb{F}_{11}$ que tiene como matriz generadora

$$G = \begin{pmatrix} 3 & 1 & 1 & 5 & 0 \\ 0 & -3 & 0 & 5 & 1 \\ 1 & 5 & 0 & 4 & 1 \end{pmatrix}.$$

a) (0,5 punto) Calcula su matriz de paridad.

b) (0,5 punto) Calcula los parámetros del código.

c) (0,5 punto) ¿Es un código perfecto? ¿Es un código MDS? ¿Que valor tiene $A_{11}(5,3)$?

d) (1,5 puntos) Empleamos este código para transmitir palabras castellanas escritas con el alfabeto que tiene 36 letras. Las 10 primeras letras corresponden a los números $0,\ldots,9$ y las 26 restantes al alfabeto castellano sin $\tilde{\text{N}}$: 10=A,...,35=Z. Hacemos corresponder a cada digrafo un vector de $\mathbb{F}_{11}^3$: primero vemos el digrafo como un número de dos cifras en base 36, después lo convertimos en un número entero entre 0 y $1295 = (36)^2 - 1$ y a continuación escribimos este número en base 11:

$$00 = (0,0,0), 01 = (0,0,1), \ldots, AA = (3,0,7), \ldots, ZZ = (10,7,8).$$

Antes de transmitir el digrafo que corresponde al vector $x = (x_1, x_2, x_3)$ se codifica como $xG \in \mathbb{F}_{11}^5$.

Sabiendo que se trata de una ciudad ¿qué leerías si recibieras el siguiente mensaje

$$(6,5,0,1,5); (2,0,0,7,2); (5,6,5,-1,1)?$$