TEORÍA DE CÓDIGOS Y CRIPTOGRAFÍA | **Examen Final : 25-1-2012**

SOLUCIONES

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.

Solución: Sea $f = g_2 \circ g_1 : (\mathbb{Z}/30\mathbb{Z})^2 \to (\mathbb{Z}/30\mathbb{Z})^2$. Por definición se tiene

$$f(x,y) = g_2\left(\left(\begin{smallmatrix} 3 & 1 \\ 17 & 2 \end{smallmatrix}\right)\left(\begin{smallmatrix} x \\ y \end{smallmatrix}\right) + \left(\begin{smallmatrix} 2 \\ 3 \end{smallmatrix}\right)\right) = \left(\begin{smallmatrix} 1 & 1 \\ 19 & 2 \end{smallmatrix}\right)\left(\left(\begin{smallmatrix} 3 & 1 \\ 17 & 2 \end{smallmatrix}\right)\left(\begin{smallmatrix} x \\ y \end{smallmatrix}\right) + \left(\begin{smallmatrix} 2 \\ 3 \end{smallmatrix}\right)\right) = \left(\begin{smallmatrix} 20 & 3 \\ 1 & 23 \end{smallmatrix}\right)\left(\begin{smallmatrix} x \\ y \end{smallmatrix}\right) + \left(\begin{smallmatrix} 5 \\ 14 \end{smallmatrix}\right).$$

Es decir, nuestro criptosistema es matricial afín sobre digrafos sobre $\mathbb{Z}/30\mathbb{Z}$ con $A = \left(\begin{smallmatrix} 20 & 3 \\ 1 & 23 \end{smallmatrix}\right)$ y $b = \left(\begin{smallmatrix} 5 \\ 14 \end{smallmatrix}\right)$. Así tendremos que $f^{-1}(u,v) = A^{-1}\left(\begin{smallmatrix} u \\ v \end{smallmatrix}\right) - A^{-1}b$. Es decir:

$$f^{-1}(u,v) = \left(\begin{smallmatrix} 29 & 21 \\ 17 & 20 \end{smallmatrix}\right)\left(\begin{smallmatrix} u \\ v \end{smallmatrix}\right) + \left(\begin{smallmatrix} 11 \\ 25 \end{smallmatrix}\right).$$

Ahora descifremos el mensaje:

$$\begin{aligned} f^{-1}(\text{B¿}) &= f^{-1}\left(\begin{smallmatrix} 1 \\ 28 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 28 \\ 2 \end{smallmatrix}\right) = \text{¿C} \\ f^{-1}(\text{VE}) &= f^{-1}\left(\begin{smallmatrix} 21 \\ 4 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 14 \\ 12 \end{smallmatrix}\right) = \text{OM} \\ f^{-1}(\text{MF}) &= f^{-1}\left(\begin{smallmatrix} 12 \\ 5 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 14 \\ 29 \end{smallmatrix}\right) = \text{O?} \end{aligned}$$

Así que nos el mensaje descifrado es:

¿COMO?

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

Solución: En primer lugar necesitamos calcular la clave de descifrado d. Es decir, el inverso de e módulo $\varphi(n)$. Como sabemos que $n = p \cdot q$, para algunos primos p y q, tendremos que $\varphi(n) = (p-1)(q-1)$. Por lo tanto, hemos de factorizar n. En primer lugar intentemoslo mediante fuerza bruta. Esto es, vamos a utilizar que n siempre tiene un divisor primo p menor que $\sqrt{n} < 2897$. Por lo tanto dividiendo por los primeros primos: $2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47$, observamos que podemos parar en 47, ya que divide a n. El otro divisor es 178481. Otra manera de factorizar es viendo que $n + 1 = 2^{23}$. Vamos a utilizar un resultado visto en clase que permite factorizar números de la forma $b^m - 1$ que dice que si p es un divisor primo de $b^m - 1$ entonces o bien $p | b^d - 1$ con $0 \leq d < n$ con $d | n$; o bien $p \equiv 1 \pmod{n}$, y en este último caso si $p \neq 2$ y n impar entonces se tiene $p \equiv 1 \pmod{2n}$. Vamos a aplicarlo a nuestro caso: $b = 2$, $m = 23$. Como 23 es primo la primera condición no nos dice nada. En cuanto a la segunda buscamos un primo impar p de la forma $p \equiv 1 \pmod{46}$. El primero de ellos es $p = 47$ y vemos que divide a $2^{23} - 1$. Por lo tanto hemos terminado.

Así hemos calculado $\varphi(n) = 8210080$, que nos permite calcular d mediante la identidad de Bezout $ed + a\varphi(n) = 1$ utilizando el Algoritmo de Euclides, ya que $mcd(e, \varphi(n)) = 1$. En nuestro caso obtenemos $d = 7$. Ya tenemos la clave de descifrado.

Descifremos el mensaje. En primer lugar tenemos que calcular el tamaño de los bloques para descifrar (y cifrar):

$$l_1 = \left\lfloor \frac{\log 8388607}{\log 30} \right\rfloor = 4 \qquad \text{y} \qquad l_2 = \left\lceil \frac{\log 8388607}{\log 30} \right\rceil = 5.$$

Así si denotamos por f la función de cifrado se tendrá:

$$\begin{array}{ccccccc} \mathbb{Z}/30^4\mathbb{Z} & \hookrightarrow & \mathbb{Z}/8388607\mathbb{Z} & \xrightarrow{f} & \mathbb{Z}/8388607\mathbb{Z} & \hookrightarrow & \mathbb{Z}/30^5\mathbb{Z} \\ x = a_3 30^3 + a_2 30^2 + a_1 30 + a_0 & \mapsto & x & \mapsto & y \equiv x^{5864343} \pmod{8388607} & \mapsto & y = b_4 30^4 + b_3 30^3 + b_2 30^2 + b_1 30 + b_0 \end{array}$$

De forma equivalente la inversa:

$$\begin{array}{ccccccc} \mathbb{Z}/30^5\mathbb{Z} & \to & \mathbb{Z}/8388607\mathbb{Z} & \xrightarrow{f^{-1}} & \mathbb{Z}/8388607\mathbb{Z} & \to & \mathbb{Z}/30^4\mathbb{Z} \\ y = b_4 30^4 + b_3 30^3 + b_2 30^2 + b_1 30 + b_0 & \mapsto & y & \mapsto & x \equiv y^7 \pmod{8388607} & \mapsto & x = a_3 30^3 + a_2 30^2 + a_1 30 + a_0 \end{array}$$

Recordemos que para calcular $y^7 \pmod{8388607}$ se hace por cuadrados iterados, utilizando que $7 = 1 + 2^1 + 2^2$. Así obtenemos:

$$f^{-1}(\text{GTAF?}) = f^{-1}(6{\cdot}30^4{+}19{\cdot}30^3{+}0{\cdot}30^2{+}5{\cdot}30{+}29) = f^{-1}(5373179) \equiv 5373179^7 \pmod{8388607} \equiv 324360 \pmod{8388607}$$

Ahora escribimos $324360 = 12 \cdot 30^3 + 0 \cdot 30^2 + 12 \cdot 30 + 0$, que corresponde al mensaje descifrado que es

MAMA

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.

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

Solución: Los parámetros de un $(n, M, d)_q$-código representan: n la longitud de sus elementos, M el cardinal, d la distancia de Hamming mínima entre elementos del código y q el cardinal de $\mathcal{A}$, el alfabeto en donde está escrito el código. El código será lineal si forma un subespacio vectorial de $\mathcal{A}^n$, una condición necesaria es que $\mathcal{A}$ sea un cuerpo y que M sea una potencia de q. Así tenemos

• C_1 es un $(2, 9, 1)_3$-código lineal ya que $C_1 = (\mathbb{F}_3)^2$. Una matriz generadora de C_1 sería la matriz identidad 2x2. Como $C_1 = (\mathbb{F}_3)^2$ tenemos que la dimensión del código dual de C_1 es cero, es decir que esta compuesto por el elemento 00.

• C_2 es un $(2, 4, 1)_7$-código. En este caso no es lineal, ya que aunque el alfabeto es un cuerpo (en este caso $\mathbb{F}_7$) se tiene que su cardinal es 4 que no es una potencia de 7 y por lo tanto no puede ser un subespacio vectorial de $(\mathbb{F}_7)^2$.

• C_3 es un $(5, 10, 5)_{10}$-código. Tampoco es lineal. En este caso porque $\mathbb{Z}/10\mathbb{Z}$ no es un cuerpo.

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

Solución: En primer lugar podríamos ver si no existe utilizando la cota de Singleton o la cota de Hamming. Recordemos que la cota de Singleton en el caso de $[n, k, d]_q$-códigos dice: $k \leq n - d + 1$. En nuestro caso tenemos $9 \leq 11 - 3 + 1 = 9$. Así que no podemos descartar su existencia. Ahora utilicemos la cota de Hamming. Recordemos que si tenemos un $[n, k, d]_q$-código con $d = 2t + 1$ ó $d = 2t + 2$, este ha de cumplir:

$$\sum_{i=0}^{t} \binom{n}{i} (q-1)^i \leq q^{n-k}.$$

En nuestro caso tenemos $1 + 11 \cdot 22 = 243 < 23^{11-9} = 529$. Así que esta cota tampoco nos permite descartar la existencia de un $[11, 9, 3]_{23}$-código.

Ahora veamos si la cota de Gilbert–Varshamov nos dice algo. Recordemos que esta cota nos dice que si q es una potencia de un primo y

$$\sum_{i=0}^{d-2} \binom{n-1}{i} (q-1)^i < q^{n-k},$$

entonces existe un $[n, k, d]_q$-código. En nuestro caso tenemos $1 + 10 \cdot 22 = 221 < 23^{11-9} = 529$. Así que tenemos que existe un $[11, 9, 3]_{23}$-código.

Vamos a construir una matriz de paridad H de un $[11, 9, 3]_{23}$-código. Como $n = 11$ y $k = 9$ se tiene que una matriz de paridad será de orden 2x11. Así vamos a imitar la construcción de los códigos de Hamming para construir H. Es decir, queremos construir una matriz con 2 filas y 11 columnas de tal forma que ninguna de las columnas sea nula, ni ningún par de columnas sea proporcional. Observar que con las condiciones anteriores tenemos que las 2 filas serán independientes y que la distancia del código del que H es la matriz de paridad será 3. Así obtenemos un ejemplo de matriz de paridad de un $[11, 9, 3]_{23}$-código:

$$H = \begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \end{pmatrix}.$$

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

Solución 1: Tenemos que G tiene sólo 3 filas y el cuerpo base es $\mathbb{F}_2$. Por lo tanto $|C_G| = 2^3$ y podemos construir todas las palabras del código de forma sencilla mediante $u \cdot G$ donde $u \in (\mathbb{F}_2)^3$. En este caso la codificación de los 8 puntos cardinales es:

	i	u	$u \cdot G$
N	0	000	000000
NE	1	001	011000
E	2	010	010110
SE	3	011	001110
S	4	100	110000
SO	5	101	101000
O	6	110	100110
NO	7	111	111110

Ahora podemos calcular la distancia del código utilizando que como es lineal se tiene que $d(C_G) = w(C_G)$. En este caso es fácil ver que el peso mínimo es 2, obtenemos que C_G es un $[6, 3, 2]_2$-código. Con lo que se obtiene que es un código 1-detector y 0-corrector. Esto es, detecta todos los errores simples. Observar que si es 0-corrector no quiere decir que no haya errores que pueda corregir.

Ahora veamos que ha de hacer el robot en las distintas transmisiones:
• 111110: En este caso como $111110 \in C_G$ y corresponde a NO el robot se moverá hacia el NO.
• 001000: En primer lugar vemos que $001000 \notin C_G$. Ahora observamos que al menos las palabras del código 000000 y 011000 están a distancia 1 de 001000. Por lo tanto el robot no puede decodificar la transmisión recibida y tiene que pedir retransmisión desde la tierra.
• 000001: De nuevo tenemos $000001 \notin C_G$. Pero en este caso observamos que 000000 es la única palabra del código a distancia 1 de 000001. Por lo tanto el robot corrige el error y decodifica como 000000 y se dirige a N.

Solución 2: Como estamos tratando con un código lineal vamos a intentar decodificar utilizando el método de los síndromes. Para ello en primer lugar mediante reducción Gaussiana sólo en las filas obtenemos una matriz estándar y de ella obtenemos la siguiente matriz de paridad del código C_G:

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

Vemos que H no tiene ninguna columna formada por ceros, pero las tres primeras columnas son iguales. De lo que deducimos que la distancia del código es 2. Por lo tanto, C_G es un $[6, 3, 2]_2$-código. Con lo que se obtiene que es un código 1-detector y 0-corrector. Esto es, detecta todos los errores simples. Observar que si es 0-corrector no quiere decir que no haya errores que pueda corregir.
Ahora veamos que ha de hacer el robot en las distintas transmisiones:
• 111110: Calculamos su síndrome $s_H(111110) = 000$. Por lo tanto $111110 \in C_G$, que corresponde a NO el robot se moverá hacia el NO.
• 001000: En este caso $s_H(001000) = 110$, por lo tanto $001000 \notin C_G$ y vemos que $s_H(001000)$ corresponde a las tres primeras columnas de H. Por lo tanto el robot no puede decodificar la transmisión recibida y tiene que pedir retransmisión desde la tierra.
• 000001: En esta última transmisión tenemos $s_H(000001) = 001$. De nuevo tenemos $000001 \notin C_G$. Pero en este caso observamos que $s_H(000001)$ corresponde a una única columna, esto es a la última columna. Por lo tanto para decodificar calculamos $000001 - 000001 = 000000$. Por lo tanto el robot corrige el error y decodifica como 000000 y se dirige a N.