TEORÍA DE CÓDIGOS Y CRIPTOGRAFÍA | **Examen 8-9-2011**

SOLUCIONES

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

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`.

Solución: Comencemos por el cifrado matricial afín. Sea $f = f_{A,b} : (\mathbb{Z}/26\mathbb{Z})^2 \longrightarrow (\mathbb{Z}/26\mathbb{Z})^2$ la función de cifrado. Esto es, para $x \in (\mathbb{Z}/26\mathbb{Z})^2$, se define como $f(x) = Ax + b$, donde $A = \left(\begin{smallmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{Z}/26\mathbb{Z})$ y $b = \left(\begin{smallmatrix} b_1 \\ b_2 \end{smallmatrix}\right) \in (\mathbb{Z}/26\mathbb{Z})^2$. Se nos pide $f(\texttt{MADRID}) = \texttt{BILBAO}$. Es decir:

$$f(\texttt{MA}) = \texttt{BI} \;\Rightarrow\; A\left(\begin{smallmatrix} 12 \\ 0 \end{smallmatrix}\right) + b = \left(\begin{smallmatrix} 1 \\ 8 \end{smallmatrix}\right) \;\Rightarrow\; \begin{cases} 12a_{11} + b_1 = 1 \\ 12a_{21} + b_2 = 8 \end{cases} \quad (1)$$

$$f(\texttt{DR}) = \texttt{LB} \;\Rightarrow\; A\left(\begin{smallmatrix} 3 \\ 17 \end{smallmatrix}\right) + b = \left(\begin{smallmatrix} 11 \\ 1 \end{smallmatrix}\right) \;\Rightarrow\; \begin{cases} 3a_{11} + 17a_{12} + b_1 = 11 \\ 3a_{21} + 17a_{22} + b_2 = 1 \end{cases} \quad (2)$$

$$f(\texttt{ID}) = \texttt{AO} \;\Rightarrow\; A\left(\begin{smallmatrix} 8 \\ 3 \end{smallmatrix}\right) + b = \left(\begin{smallmatrix} 0 \\ 14 \end{smallmatrix}\right) \;\Rightarrow\; \begin{cases} 8a_{11} + 3a_{12} + b_1 = 0 \\ 8a_{21} + 3a_{22} + b_2 = 14 \end{cases} \quad (3)$$

Los sistemas de ecuaciones (1), (2) y (3) forman un sistema de 6 ecuaciones lineales con 6 incognitas $(a_{11}, a_{12}, a_{21}, a_{22}, b_1, b_2)$ compatible determinado cuya solución en $\mathbb{Z}/26\mathbb{Z}$ es:

$$A = \left(\begin{smallmatrix} 17 & 5 \\ 23 & 24 \end{smallmatrix}\right) \qquad \text{y} \qquad b = \left(\begin{smallmatrix} 5 \\ 18 \end{smallmatrix}\right)$$

Por lo tanto, $f\left(\begin{smallmatrix} x_1 \\ x_2 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 17 & 5 \\ 23 & 24 \end{smallmatrix}\right)\left(\begin{smallmatrix} x_1 \\ x_2 \end{smallmatrix}\right) + \left(\begin{smallmatrix} 5 \\ 18 \end{smallmatrix}\right)$. Ahora veamos si existe $g : \mathbb{Z}/26^2\mathbb{Z} \longrightarrow \mathbb{Z}/26^2\mathbb{Z}$ cifrado afín. Es decir, para $x \in \mathbb{Z}/26^2\mathbb{Z}$, se define como $g(x) \equiv ax + b \pmod{26^2}$, donde $(a, 26) = 1$. Se nos pide $g(\texttt{MADRID}) = \texttt{BILBAO}$. Es decir:

$$g(\texttt{MA}) = \texttt{BI} \;\Rightarrow\; a(12 \cdot 26 + 0) + b \equiv 1 \cdot 26 + 8 \pmod{26^2} \;\Rightarrow\; 312a + b \equiv 34 \pmod{26^2} \quad (1)$$

$$g(\texttt{DR}) = \texttt{LB} \;\Rightarrow\; a(3 \cdot 26 + 17) + b \equiv 11 \cdot 26 + 1 \pmod{26^2} \;\Rightarrow\; 95a + b \equiv 287 \pmod{26^2} \quad (2)$$

$$g(\texttt{ID}) = \texttt{AO} \;\Rightarrow\; a(8 \cdot 26 + 3) + b \equiv 0 \cdot 26 + 14 \pmod{26^2} \;\Rightarrow\; 211a + b \equiv 14 \pmod{26^2} \quad (3)$$

El sistema formado por las ecuaciones (1), (2) y (3) forman un sistema de 3 ecuaciones lineales con 2 incognitas (a y b) imcompatible en $\mathbb{Z}/26^2\mathbb{Z}$. Por lo tanto no existe g que mande `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?**

Solución 1: En primer lugar tenemos que calcular el tamaño de los bloques para descifrar (y cifrar) módulo n_i. Se obtiene que para $i = 1, 2, 3$:

$$l_1 = \left\lfloor \frac{\log n_i}{\log 26} \right\rfloor = 5 \qquad \text{y} \qquad l_2 = \left\lceil \frac{\log n_i}{\log 26} \right\rceil = 6.$$

Por lo tanto cada c_i corresponde a un único bloque. Así tenemos

$$\begin{aligned} c_1 &= \texttt{EEWNRB} = 4 + 4 \cdot 26 + 22 \cdot 26^2 + 13 \cdot 26^3 + 17 \cdot 26^4 + 1 \cdot 26^5 = 19893436 \\ c_2 &= \texttt{MEEPKA} = 12 + 4 \cdot 26 + 4 \cdot 26^2 + 15 \cdot 26^3 + 10 \cdot 26^4 + 0 \cdot 26^5 = 4836220 \\ c_3 &= \texttt{NGQGNE} = 13 + 6 \cdot 26 + 16 \cdot 26^2 + 6 \cdot 26^3 + 13 \cdot 26^4 + 4 \cdot 26^5 = 53582633 \end{aligned}$$

Denotemos por m la palabra enviada. Como el exponente de cifrado $e = 3$ es común a mis tres amigos tenemos que $c_i \equiv m^3 \pmod{n_i}$ para $i = 1, 2, 3$. Ahora, podemos ver que n_1, n_2, n_3 son primos entre si. Aplicando el Teorema Chino del Resto podemos calcular $m^3 \pmod{n_1 n_2 n_3}$. Esto es:

$$\left\{ \begin{array}{l} m^3 \equiv 19893436 \pmod{n_1} \\ m^3 \equiv 4836220 \pmod{n_2} \\ m^3 \equiv 53582633 \pmod{n_3} \end{array} \right\} \qquad \Rightarrow \qquad m^3 \equiv 53582633 \pmod{n_1 n_2 n_3}\,.$$

Ahora, como $m < n_i$ para $i = 1, 2, 3$, tenemos que $m^3 < n_1 n_2 n_3$. Es decir, 53582633 es un cubo perfecto sobre $\mathbb{Z}$. Es decir:

$$m = \sqrt[3]{53582633} = 377 = 13 + 14 \cdot 26.$$

Concluyendo que la palabra enviada es $m =$ `NO`.

Solución 2: Necesitamos calcular la clave secreta de alguno de los amigos. Vamos a verlo con el segundo de ellos. Para ellos queremos factorizar $n_2 = 48746413$. Utilizando el método de Fermat: Sea $Q(x) = x^2 - n_2$ y $x_0 = \lceil \sqrt{n_2} \rceil = 6982$. Vamos a buscar un entero positivo k tal que $Q(x_0 + k)$ sea un cuadrado.

$$Q(x_0) = 1911, \qquad Q(x_0 + 1) = 15876 = 126^2\,.$$

Por lo tanto, si tomamos $x = x_0 + 1 = 6983$ e $y = 126$ obtenemos la factorización

$$n_2 = (x + y)(x - y) = 7109 \cdot 6857.$$

Como nos aseguran que n_2 es un número RSA tenemos la factorización en primos de n_2.
Una vez calculado la factorización de n_2 para calcular la clave secreta d_2, es suficiente con calcular:

$$d = e^{-1} \pmod{\varphi(n_2)} = \frac{1}{3} \pmod{48732448} = 32488299.$$

Ahora calculamos el tamaño de los bloques para descifrar (y cifrar) módulo n_2:

$$l_1 = \left\lfloor \frac{\log n_2}{\log 26} \right\rfloor = 5 \qquad \text{y} \qquad l_2 = \left\lceil \frac{\log n_2}{\log 26} \right\rceil = 6.$$

Por lo tanto c_2 corresponde a un único bloque. Así tenemos

$$c_2 = \texttt{MEEPKA} = 12 + 4 \cdot 26 + 4 \cdot 26^2 + 15 \cdot 26^3 + 10 \cdot 26^4 + 0 \cdot 26^5 = 4836220$$

El siguiente paso es calcular $m = c_2^{d_2} \pmod{n_2}$ mediante cuadrados iterados, obteniendo $m = 377 = 13 + 14 \cdot 26$. Concluyendo que la palabra enviada es $m =$ `NO`.

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.

Solución: El código que genera la matriz $\mathcal{G}$ es un código lineal sobre $\mathbb{F}_5$ con n igual al número de columnas y M igual a 5 elevado al número de filas. Es decir, $n = 6$ y $M = 5^3 = 125$. Ahora nos falta por calcular la distancia mínima del código. Para ello vamos a calcular una matriz de paridad. Como $\mathcal{G}$ está dada en forma estándar, es decir $\mathcal{G} = (I_3|A)$, tenemos que una matriz de paridad es de la forma $H = (-A^t|I_3)$. Así nos queda:

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

Denotemos por H_i la columna i-ésima de H. Vemos que ninguna de las columnas es cero. Por lo tanto $d \geq 2$. Ahora se observa que $H_3 = -H_1$. Por lo tanto $d = 2$. Así, hemos visto que el código que genera $\mathcal{G}$ es un código $[6, 3, 2]_5$. De lo que se deduce que es un código 0-corrector, ya que $d = 2 = 2 \cdot 0$.

(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?

Solución: Hemos demostrado en el apartado anterior que la longitud de las palabras código es 6. Por lo tanto, el código generado por $\mathcal{G}$ envía vectores de $\mathbb{F}_5^3$ en vectores de $\mathbb{F}_5^6$. Es decir, se tiene

$$(x_1, x_2, x_3)\mathcal{G} = (x_1, x_2, x_3, y_1, y_2, y_3),$$

donde (y_1, y_2, y_3) es la redundancia. Así, a cada letra que aparece en las tablas anteriores le hace corresponder un digrafo escrito con letras de las anteriores tablas. Así el mensaje recibido hay que dividirlo en digrafos, para posteriormente escribirlo como vectores de $\mathbb{F}_5^6$. En nuestro caso:

$$\left.\begin{array}{l} \texttt{N} \leftrightarrow 78 = 3 + 0 \cdot 5 + 3 \cdot 5^2 \leftrightarrow (3, 0, 3) \\ \texttt{I} \leftrightarrow 73 = 3 + 4 \cdot 5 + 2 \cdot 5^2 \leftrightarrow (3, 4, 2) \end{array}\right\} \Leftrightarrow \texttt{NI} \leftrightarrow (3, 0, 3, 3, 4, 2)$$

$$\left.\begin{array}{l} \texttt{d} \leftrightarrow 100 = 0 + 0 \cdot 5 + 4 \cdot 5^2 \leftrightarrow (0, 0, 4) \\ \texttt{W} \leftrightarrow 87 = 2 + 2 \cdot 5 + 3 \cdot 5^2 \leftrightarrow (2, 2, 3) \end{array}\right\} \Leftrightarrow \texttt{dW} \leftrightarrow (0, 0, 4, 2, 2, 3)$$

Hemos visto en el apartado (a) que el código que genera $\mathcal{G}$ (denotado por $C_{\mathcal{G}}$) es 1-corrector. Si nos mandan una palabra código $c \in C_{\mathcal{G}}$ y hemos recibido $x = c + e$, donde $e \in \mathbb{F}_5^6$ es el error, si $\omega(e) \leq 1$ el código $C_{\mathcal{G}}$ corregirá correctamente. Si $\omega(e) = 0$ esto quiere decir que $c = x \in C_{\mathcal{G}}$. Si $\omega(e) = 1$, entonces $e = \alpha \cdot e_i$ para $i \in \{1, 2, 3, 4, 5, 6\}$, e_i un vector de la base canónica de $\mathbb{F}_5^6$ y $\alpha \in \mathbb{F}_5$. Así tendríamos que $c = x - \alpha \cdot e_i$. ¿Cómo calcular i? Respuesta: Aplicando síndromes. Recordemos la definición del síndrome de $x \in \mathbb{F}_5^6$ con respecto a una matriz de paridad H: $s_H(x) := x \cdot H^t$.

En nuestro caso tendríamos:

$$s_H(x) = s_H(c+e) = s_H(c) + s_H(e) = s_H(e) = \alpha \cdot s_H(e_i) = \alpha \cdot {H_i}^t$$

donde H_i denota la columna i-ésima de H.
Denotemos por $x_1 = (3,0,3,3,4,2)$ y $x_2 = (0,0,4,2,2,3)$. Vamos a decodificar utilizando el método de los síndromes:

$$s_H(x_1) = (3,0,3,3,4,2)H^t = (3,4,2) = -1 \cdot {H_2}^t \quad \Longrightarrow \quad c_1 = x_1 - (-1)\cdot e_2 \quad \Longrightarrow \quad c_1 = (3,1,3,3,4,2)\,,$$

$$s_H(x_2) = (0,0,4,2,2,3)H^t = (3,4,2) = -1 \cdot {H_2}^t \quad \Longrightarrow \quad c_2 = x_2 - (-1)\cdot e_2 \quad \Longrightarrow \quad c_2 = (0,1,4,2,2,3)\,.$$

Como $\mathcal{G}$ esta en forma estandar, tenemos que si $(x_1,x_2,x_3,x_4,x_5,x_6) \in C_{\mathcal{G}}$, entonces la letra codificada corresponde al número $x_1 + x_2 5 + x_3 5^2$ en las tablas ASCII anteriores. En nuestro caso obtenemos:

$$\begin{array}{lllll} c_1 = (3,1,3,3,4,2) & \Longrightarrow & n_1 = 3 + 1\cdot 5 + 3\cdot 5^2 = 83 & \Longrightarrow & \texttt{S} \\ c_2 = (0,1,4,2,2,3) & \Longrightarrow & n_2 = 0 + 1\cdot 5 + 4\cdot 5^2 = 105 & \Longrightarrow & \texttt{i} \end{array}$$

Por lo tanto la palabra enviada es:

`Si.`

4. Denotamos por $A_q(n,d)$ el máximo M tal que existe un $(n,M,d)_q$-código.
(a) Calcular $A_{11}(12,3)$.

Solución: El código de Hamming p-ario de orden r, que denotamos por $\mathcal{H}am(r,p)$, es un codigo lineal perfecto sobre $\mathbb{F}_p$ con parámetros

$$n = \frac{p^r - 1}{p-1}\,, \qquad k = n - r \qquad d = 3.$$

Escojamos $p = 11$ y $r = 2$. Entonces $n = \frac{11^2-1}{10} = 12$. Por lo tanto, el código $\mathcal{H}am(2,11)$ tiene $n = 12$, $d = 3$ y es perfecto, lo que demuestra:

$$A_{11}(12,3) = 11^{12-2} = 11^{10}.$$

(b) Describir las palabras código de un $(12,M,3)_{11}$-código con $M = A_{11}(12,3)$.

Solución: Una matriz de paridad del código $\mathcal{H}am(2,11)$ es una matriz cuyas columnas son las 12 palabras no nulas de $\mathbb{F}_{11}^2$ módulo producto por escalares en $\mathbb{F}_{11}$:

$$H = \begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \end{pmatrix}.$$

Así que tenemos que $H = (I_2|B)$ con $B = \left(\begin{smallmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \end{smallmatrix}\right)$ por lo tanto la matriz $G = (-B^t|I_{10})$ es una matriz generadora del código $\mathcal{H}am(2,11)$.

Así tenemos dos posibles descripciones de las palabras código de $\mathcal{H}am(2,11)$:

- $\mathcal{H}am(2,11) = \{x \in \mathbb{F}_{11}^{12} \,|\, x \cdot H^t = 0\}$.
- $\mathcal{H}am(2,11) = \{u \cdot G \,|\, u \in \mathbb{F}_{11}^{10}\}$.