TEORÍA DE CÓDIGOS Y CRIPTOGRAFÍA | **Examen Final 27-01-2011**

SOLUCIONES

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

El alfabeto utilizado 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. Recibimos un mensaje cifrado que sabemos comienza ZQCNGNRZOCVG y termina FGRZGO. Hemos averiguado que han utilizado un cifrado matricial afín sobre vectores de $(\mathbb{Z}/26\mathbb{Z})^2$. Más aún, el texto comienza con el título de una famosa canción y termina con el autor. Pero aún hemos conseguido más información: el autor de la canción es SERRAT. ¿Cuál es el título de la canción? Calcular la transformación afín de cifrado (matriz y vector).

Solución: 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 $A \in \mathrm{GL}_2(\mathbb{Z}/26\mathbb{Z})$ y $b \in (\mathbb{Z}/26\mathbb{Z})^2$. Sabemos

$$\begin{aligned} f(SE) = FG \quad &\Rightarrow \quad A\left(\begin{smallmatrix}18\\4\end{smallmatrix}\right) + b = \left(\begin{smallmatrix}5\\6\end{smallmatrix}\right) \qquad (1)\\ f(RR) = RZ \quad &\Rightarrow \quad A\left(\begin{smallmatrix}17\\17\end{smallmatrix}\right) + b = \left(\begin{smallmatrix}17\\25\end{smallmatrix}\right) \qquad (2)\\ f(AT) = GO \quad &\Rightarrow \quad A\left(\begin{smallmatrix}0\\19\end{smallmatrix}\right) + b = \left(\begin{smallmatrix}6\\14\end{smallmatrix}\right) \qquad (3)\end{aligned}$$

Calculando (2) − (1) y (3) − (1) obtenemos $A\left(\begin{smallmatrix}25 & 8\\13 & 15\end{smallmatrix}\right) = \left(\begin{smallmatrix}12 & 1\\19 & 8\end{smallmatrix}\right)$. Sea $P = \left(\begin{smallmatrix}25 & 8\\13 & 15\end{smallmatrix}\right)$ y $C = \left(\begin{smallmatrix}12 & 1\\19 & 8\end{smallmatrix}\right)$. Como $\det(P) = 11$ es un invertible en el anillo $\mathbb{Z}/26\mathbb{Z}$, tenemos que $P \in \mathrm{GL}_2(\mathbb{Z}/26\mathbb{Z})$ y existe P^{-1}. Por lo tanto:

$$A = C \cdot P^{-1} = \left(\begin{smallmatrix}12 & 1\\19 & 8\end{smallmatrix}\right)\left(\begin{smallmatrix}25 & 4\\13 & 7\end{smallmatrix}\right) = \left(\begin{smallmatrix}1 & 3\\7 & 2\end{smallmatrix}\right).$$

De la ecuación (1) obtenemos $b \in (\mathbb{Z}/26\mathbb{Z})^2$:

$$b = \left(\begin{smallmatrix}5\\6\end{smallmatrix}\right) - A\left(\begin{smallmatrix}18\\4\end{smallmatrix}\right) = \left(\begin{smallmatrix}5\\6\end{smallmatrix}\right) - \left(\begin{smallmatrix}1 & 3\\7 & 2\end{smallmatrix}\right)\left(\begin{smallmatrix}18\\4\end{smallmatrix}\right) = \left(\begin{smallmatrix}1\\2\end{smallmatrix}\right).$$

Para obtener la función descifrado, observar que $f^{-1}(y) = A'y + b'$ donde $A' = A^{-1}$ y $b' = -A^{-1}b$. Por lo tanto:

$$f\left(\begin{smallmatrix}x_1\\x_2\end{smallmatrix}\right) = \left(\begin{smallmatrix}1 & 3\\7 & 2\end{smallmatrix}\right)\left(\begin{smallmatrix}x_1\\x_2\end{smallmatrix}\right) + \left(\begin{smallmatrix}1\\2\end{smallmatrix}\right) \qquad \text{y} \qquad f^{-1}\left(\begin{smallmatrix}y_1\\y_2\end{smallmatrix}\right) = \left(\begin{smallmatrix}4 & 7\\25 & 15\end{smallmatrix}\right)\left(\begin{smallmatrix}y_1\\y_2\end{smallmatrix}\right) + \left(\begin{smallmatrix}8\\23\end{smallmatrix}\right).$$

Ahora descifremos el mensaje:

$$\begin{aligned} f^{-1}(ZQ) = f^{-1}\left(\begin{smallmatrix}25\\16\end{smallmatrix}\right) = \left(\begin{smallmatrix}12\\4\end{smallmatrix}\right) &= ME\\ f^{-1}(CN) = f^{-1}\left(\begin{smallmatrix}2\\13\end{smallmatrix}\right) = \left(\begin{smallmatrix}3\\8\end{smallmatrix}\right) &= DI\\ f^{-1}(GN) = f^{-1}\left(\begin{smallmatrix}6\\13\end{smallmatrix}\right) = \left(\begin{smallmatrix}19\\4\end{smallmatrix}\right) &= TE\\ f^{-1}(RZ) = f^{-1}\left(\begin{smallmatrix}17\\25\end{smallmatrix}\right) = \left(\begin{smallmatrix}17\\17\end{smallmatrix}\right) &= RR\\ f^{-1}(OC) = f^{-1}\left(\begin{smallmatrix}14\\2\end{smallmatrix}\right) = \left(\begin{smallmatrix}0\\13\end{smallmatrix}\right) &= AN\\ f^{-1}(VG) = f^{-1}\left(\begin{smallmatrix}21\\6\end{smallmatrix}\right) = \left(\begin{smallmatrix}4\\14\end{smallmatrix}\right) &= EO\end{aligned}$$

La canción es MEDITERRANEO.

2. Mi clave pública RSA es $(n, e) = (9797, 1477)$. Alguien ha utilizado esta clave pública para mandarme el siguiente mensaje:

NIWJRJHXAIBNNDC

Pero como soy muy despistado, no encuentro donde guardé mi clave secreta para poder descifrar el mensaje. Calcula mi clave secreta y descifra el mensaje.

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. Utilicemos el Método de Fermat. Sea $Q(x) = x^2 - n = x^2 - 9797$. Como la parte entera de $\sqrt{9797}$ es 98, tomamos $x = 99$: $Q(99) = 4 = 2^2$. Por lo tanto,

$$9797 = (99-2)(99+2) = 97 \cdot 101.$$

Así hemos calculado $\varphi(n) = 9600$. Para calcular el inverso de $e = 1477$ módulo 9600 vamos a utilizar el Algoritmo de Euclides:

$$\begin{aligned} 9600 &= 1477 \cdot 6 + 738, \\ 1477 &= 738 \cdot 2 + 1. \end{aligned}$$

De lo que se deduce:

$$1 = 1477 - 2 \cdot 738 = 1477 - 2(9600 - 1477 \cdot 6) = 13 \cdot 1477 - 2 \cdot 9600.$$

Concluyendo que $d = 13$. Ya tenemos mi clave de descifrado.

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

$$l_1 = \left\lfloor \frac{\log 9797}{\log 26} \right\rfloor = 2 \qquad \text{y} \qquad l_2 = \left\lceil \frac{\log 9797}{\log 26} \right\rceil = 3.$$

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

$$\begin{array}{ccccccc} \mathbb{Z}/26^2\mathbb{Z} & \hookrightarrow & \mathbb{Z}/9797\mathbb{Z} & \xrightarrow{f} & \mathbb{Z}/9797\mathbb{Z} & \hookrightarrow & \mathbb{Z}/26^3\mathbb{Z} \\ x = a_1 26 + a_0 & \mapsto & x & \mapsto & y \equiv x^{1477} \pmod{9797} & \mapsto & y = b_2 26^2 + b_1 26 + b_0 \end{array}$$

De forma equivalente la inversa:

$$\begin{array}{ccccccc} \mathbb{Z}/26^3\mathbb{Z} & \to & \mathbb{Z}/9797\mathbb{Z} & \xrightarrow{f^{-1}} & \mathbb{Z}/9797\mathbb{Z} & \to & \mathbb{Z}/26^3\mathbb{Z} \\ y = b_2 26^2 + b_1 26 + b_0 & \mapsto & y & \mapsto & x \equiv y^{13} \pmod{9797} & \mapsto & x = a_1 26 + a_0 \end{array}$$

Recordemos que para calcular $y^{13} \pmod{9797}$ lo haremos por cuadrados iterados: como $13 = 1 + 2^2 + 2^3$ tendremos:

$$y^{13} = y \cdot y^{2^2} \cdot y^{2^3} \Longrightarrow \left\{ \begin{array}{l} y_0 \equiv y \pmod{9797} \\ y_1 \equiv y_0^2 \pmod{9797} \\ y_2 \equiv y_1^2 \pmod{9797} \\ y_3 \equiv y_2^2 \pmod{9797} \end{array} \right\} \ , \ \left\{ \ w_0 = y_0 \cdot y_2 \pmod{9797} \ \right\} \Longrightarrow y^{13} \equiv w_0 \cdot y_3 \pmod{9797}.$$

Aplicando el anterior algoritmo a nuestro texto cifrado, recordando que los bloques son de longitud 3, tenemos:

$$\begin{array}{lll} f^{-1}(\text{NIW}) = & f^{-1}(13 \cdot 26^2 + 8 \cdot 26 + 22) = f^{-1}(9018) \equiv 9018^{13} \pmod{9797} \equiv 66 \pmod{9797} \Leftrightarrow 66 = 2 \cdot 26 + 14 & = \text{CO} \\ f^{-1}(\text{JRJ}) = & f^{-1}(9 \cdot 26^2 + 17 \cdot 9 + 9) = f^{-1}(6535) \equiv 6535^{13} \pmod{9797} \equiv 327 \pmod{9797} \Leftrightarrow 327 = 12 \cdot 26 + 15 & = \text{MP} \\ f^{-1}(\text{HXA}) = & f^{-1}(7 \cdot 26^2 + 23 \cdot 26 + 0) = f^{-1}(5330) \equiv 5330^{13} \pmod{9797} \equiv 456 \pmod{9797} \Leftrightarrow 456 = 17 \cdot 26 + 14 & = \text{RO} \\ f^{-1}(\text{IBN}) = & f^{-1}(8 \cdot 26^2 + 1 \cdot 26 + 13) = f^{-1}(5447) \equiv 5447^{13} \pmod{9797} \equiv 26 \pmod{9797} \Leftrightarrow 26 = 1 \cdot 26 + 0 & = \text{BA} \\ f^{-1}(\text{NDC}) = & f^{-1}(13 \cdot 26^2 + 3 \cdot 26 + 2) = f^{-1}(8868) \equiv 8868^{13} \pmod{9797} \equiv 92 \pmod{9797} \Leftrightarrow 92 = 3 \cdot 26 + 14 & = \text{DO} \end{array}$$

El mensaje descifrado es COMPROBADO.

3. Sea C el código binario formado por las palabras $00000, 10110, 01011$ y 11101.
(i) Calcular los parámetros n, M y d del código.

Solución: En primer lugar denotemos por:

$$c_0 = 00000, \quad c_1 = 10110, \quad c_2 = 01011 \quad y \quad c_3 = 11101.$$

Hay $M = 4$ palabras código, todas ellas de longitud $n = 5$. La distancia mínima entre las palabras código es $d = 3$:

$$d(c_0, c_1) = 3, \quad d(c_0, c_2) = 3, \quad d(c_0, c_3) = 4, \quad d(c_1, c_2) = 4, \quad d(c_1, c_3) = 3, \quad d(c_2, c_3) = 3.$$

Así tenemos que C es un $(5, 4, 3)_2$-código.

(ii) ¿Es lineal? En caso afirmativo, calcular las matrices generadoras de C y su dual.

Solución: Observar que como C es binario, $M = 4$ y $c_0 = 0$, para ver que es lineal basta con ver que $c_1 + c_2 = c_3$. Así, C es un $[5, 2, 3]_2$-código.

Como c_1 y c_2 son linealmente independientes tenemos que forman una base de C. Así una matriz generadora de C es:

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

Como G está dada en forma estándar, es decir $G = (I_2|A)$, tenemos que una matriz de paridad (o lo que es lo mismo, una matriz generadora del código dual) es de la forma $H = (-A^t|I_3)$. Así nos queda:

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

(iii) ¿Es perfecto?

Solución: Utilicemos el teorema que nos asegura que si C es un $(n, M, d)_q$-código, entonces es perfecto si y solo si $d = 2t + 1$ y

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

En nuestro caso: $M = 4$, $q = 2$, $d = 2 \cdot 1 + 1$ y la ecuación anterior queda:

$$4 \cdot (1 + 5) = 24 \neq 2^5 = 32.$$

Por lo tanto, C no es perfecto.

(iv) Si recibimos la palabra $r = 00011$. Decodificar r.

Solución: La distancia de C es 3, por lo tanto es un código 1-corrector. Calculemos las distancias de r a cada una de las palabras del código:

$$d(c_0, r) = 2, \quad d(c_1, r) = 3, \quad d(c_2, r) = 1, \quad d(c_3, r) = 4.$$

Decodificando por mínima distancia tenemos que la respuesta es $c_2 = 01011$.

4. Hemos recibido una *información confidencial* que nos asegura que los números del próximo sorteo de la lotería primitiva son:

$$1152, \quad 3123, \quad 0220, \quad 0550, \quad 0004, \quad 1461.$$

Pero como podréis ver, no es todo tan fácil. Resulta que nuestra *fuente* nos ha mandado los 6 números de la combinación utilizando un código lineal sobre $\mathbb{F}_7$ que tiene la siguiente matriz generadora

$$G = \begin{pmatrix} 1 & 0 & 2 & 4 \\ 1 & 1 & 3 & 5 \end{pmatrix}.$$

Los números del 1 al 48 los ha puesto en base 7, es decir, el 1 es 01, el 2 es 02, así sucesivamente hasta el 48 que es 66 y el 49 que lo denota por 00. Así a un número $n = 7a+b$ con $a, b \in \mathbb{F}_7$ se le hace corresponder $(a, b)G \in \mathbb{F}_7^4$. Determinar la mayor cantidad de números de la *combinación ganadora*.

Solución: En primer lugar calculemos una matriz de paridad. Para ello pongamos en forma estándar la matriz G:

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

De aquí obtenemos la matriz de paridad mediante $G' = (I_2|A)$ entonces $H = (-A^t|I_2)$:

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

La distancia es $d = 3$ ya que no hay ninguna columna de ceros, tampoco hay columnas proporcionales y cualquier (basta con que hubiera uno) conjunto de 3 columnas es linealmente dependiente. Por lo tanto, C_G es 1-corrector. Si nos mandan una palabra código $c \in C_G$ y hemos recibido $x = c+e$, donde $e \in \mathbb{F}_7^4$ es el error, si $\omega(e) \leq 1$ el código C_G corregirá correctamente. Si $\omega(e) = 0$ esto quiere decir que $c = x \in C_G$. Si $\omega(e) = 1$, entonces $e = \alpha \cdot e_i$ para $i \in \{1, 2, 3, 4\}$, e_i un vector de la base canónica de $\mathbb{F}_7^4$ y $\alpha \in \mathbb{F}_7$. Así tendríamos que $c = x - \alpha \cdot e_i$. ¿Cómo calcular i? Respuesta: Aplicando síndromes. Recordemos la definición del síndrome de $x \in \mathbb{F}_7^4$ 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.

Denotemos por

$$x_1 = 1152, \quad x_2 = 3123, \quad x_3 = 0220, \quad x_4 = 0550, \quad x_5 = 0004, \quad x_6 = 1461.$$

Vamos a decodificar utilizando el método de los síndromes:

$$\begin{aligned}
s_H(x_1) = (1152)\begin{pmatrix} 5&3\\6&6\\1&0\\0&1 \end{pmatrix} = (2,4) = -1 \cdot H_1^t \quad &\Longrightarrow \quad c_1 = x_1 - (-1)\cdot e_1 \quad \Longrightarrow \quad c_1 = 2152 \\
s_H(x_2) = (3123)\begin{pmatrix} 5&3\\6&6\\1&0\\0&1 \end{pmatrix} = (2,4) = -1 \cdot H_1^t \quad &\Longrightarrow \quad c_2 = x_2 - (-1)\cdot e_1 \quad \Longrightarrow \quad c_2 = 4123 \\
s_H(x_3) = (0220)\begin{pmatrix} 5&3\\6&6\\1&0\\0&1 \end{pmatrix} = (0,5) = 5 \cdot H_4^t \quad &\Longrightarrow \quad c_3 = x_3 - 5\cdot e_4 \quad \Longrightarrow \quad c_3 = 0222 \\
s_H(x_4) = (0550)\begin{pmatrix} 5&3\\6&6\\1&0\\0&1 \end{pmatrix} = (0,2) = 2 \cdot H_4^t \quad &\Longrightarrow \quad c_1 = x_4 - 2\cdot e_4 \quad \Longrightarrow \quad c_4 = 0555 \\
s_H(x_5) = (0004)\begin{pmatrix} 5&3\\6&6\\1&0\\0&1 \end{pmatrix} = (0,4) = 4 \cdot H_4^t \quad &\Longrightarrow \quad c_1 = x_5 - 4\cdot e_4 \quad \Longrightarrow \quad c_5 = 0000 \\
s_H(x_6) = (1461)\begin{pmatrix} 5&3\\6&6\\1&0\\0&1 \end{pmatrix} = (0,0) \quad &\Longrightarrow \quad c_6 = x_6 \quad \Longrightarrow \quad c_6 = 1461
\end{aligned}$$

Ahora tenemos que calcular los números del 1 al 49 correspondientes a $c_1, \ldots, c_6$. Por definición:

$$C_G = \{u \cdot G \,|\, u \in \mathbb{F}_7^2\} = \left\{ (a,b) \begin{pmatrix} 1 & 0 & 2 & 4 \\ 1 & 1 & 3 & 5 \end{pmatrix} \,\middle|\, a, b \in \mathbb{F}_7 \right\} = \{(a+b, b, 2a+3b, 4a+5b) \,|\, a, b \in \mathbb{F}_7\}.$$

Así, si la palabra código es de la forma $t_1t_2t_3t_4$ entonces corresponde al número $n = 7(t_1 - t_2) + t_2$, donde hay que tener cuidado en elegir los representates de las clases módulo 7 de tal forma de que $t_1 - t_2 \in \{0, \ldots, 6\}$. En el caso de $c_1, \ldots, c_6$ obtenemos:

$$\begin{array}{lllll} c_1 = 2152 & \Longrightarrow & n_1 = 7(2-1)+1 & \Longrightarrow & n_1 = 8 \\ c_2 = 4123 & \Longrightarrow & n_2 = 7(4-1)+1 & \Longrightarrow & n_2 = 22 \\ c_3 = 0222 & \Longrightarrow & n_3 = 7(7-2)+2 & \Longrightarrow & n_3 = 37 \\ c_4 = 0555 & \Longrightarrow & n_4 = 7(7-5)+5 & \Longrightarrow & n_4 = 19 \\ c_5 = 0000 & \Longrightarrow & n_5 = 7(0-0)+0 & \Longrightarrow & n_5 = 49 \\ c_6 = 1461 & \Longrightarrow & n_6 = 7(8-4)+4 & \Longrightarrow & n_6 = 32 \end{array}$$

La combinación ganadora es:

$$8, \quad 19, \quad 22, \quad 32, \quad 37, \quad 49.$$

5. Denotamos por $A_q(n,d)$ el máximo M tal que existe un $(n, M, d)_q$-código. Calcular:

$$(i)\ A_q(n,1) \qquad (ii)\ A_q(n,n) \qquad (iii)\ A_2(15,3).$$

Para los apartados anteriores, dar un $(n, M, d)_q$-código con $M = A_q(n,d)$ para los respectivos parámetros.

Solución: Sea C un $(n, M, d)_q$-código. La Cota de Singleton nos dice $M \leq q^{n-d+1}$. En particular:

$$A_q(n,d) \leq q^{n-d+1}.$$

En nuestros dos primeros casos obtenemos:

$$A_q(n,1) \leq q^n \qquad \text{y} \qquad A_q(n,n) \leq q.$$

Sea $\mathcal{A}$ un alfabeto con q elementos, entonces el código:

(i) $C = \mathcal{A}^n$ es un $(n, q^n)_q$-código cuya distancia mínima es 1. Por lo tanto, $A_q(n,1) = q^n$.

(ii) $C = \mathcal{R}ep_{\mathcal{A}}(n)$ el código de repetición de longitud n sobre el alfabeto $\mathcal{A}$, es un $(n,q)_q$-código cuya distancia mínima es n. Por lo tanto, $A_q(n,n) = q$.

(iii) El código de Hamming $\mathcal{H}am(r,2)$ es un $(2^r - 1, 2^{2^r-1-r}, 3)_2$-codigo perfecto. Esto es,

$$A_2(2^r - 1, 3) = 2^{2^r-1-r}.$$

Por lo tanto, si tomamos $r = 4$ tenemos el código $\mathcal{H}am(4,2)$ y

$$A_2(15,3) = 2^{11} = 2048.$$

Una matriz de paridad del código $\mathcal{H}am(4,2)$ es una matriz cuyas columnas son las $15 = 2^4 - 1$ palabras no nulas de $\mathbb{F}_2^4$. O lo que es lo mismo, las columnas son las representaciones binaria de los números del 1 al 15:

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