TEORÍA DE CÓDIGOS Y CRIPTOGRAFÍA | **Examen Extra. : 27-6-2012**

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. Hemos entrado en el ordenador central de la OTAN y hemos obtenido que cifran sus mensajes utilizando RSA y que su clave privada es $(n, d) = (38009, 16123)$. Enviar el mensaje ASTANA suplantando a la OTAN.

Solución: Vamos a utilizar el método de Fermat. Sea $Q(x) = x^2 - n = x^2 - 38009$. Buscamos i tal que $Q(\lfloor\sqrt{n}\rfloor + i) = y^2$ para algún entero y. Vamos probando con $i = 1, 2, 3, \ldots$ y vemos que para $i = 1$ tenemos $Q(195) = 195^2 - 38009 = 4^2$. Por lo tanto los divisores de n son $195 + 4 = 199$ y $195 - 4 = 191$. Así hemos calculado $\varphi(n) = 37620$ y como sabemos que $mcd(d, \varphi(n)) = 1$, mediante el ALgoritmo de Euclides obtenemos la identidad de Bezout, que en nuestro caso resulta ser $7 \cdot 16123 - 3 \cdot 37620 = 1$. Así obtenemos que $e = 7$. Ya tenemos la clave de cifrado.
Cifremos el mensaje. En primer lugar tenemos que calcular el tamaño de los bloques para descifrar (y cifrar):

$$l_1 = \left\lfloor \frac{\log 38009}{\log 30} \right\rfloor = 3 \qquad \text{y} \qquad l_2 = \left\lceil \frac{\log 38009}{\log 30} \right\rceil = 4.$$

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

$$\begin{array}{ccccccc} \mathbb{Z}/30^3\mathbb{Z} & \hookrightarrow & \mathbb{Z}/38009\mathbb{Z} & \xrightarrow{f} & \mathbb{Z}/38009\mathbb{Z} & \hookrightarrow & \mathbb{Z}/30^4\mathbb{Z} \\ x = a_2 30^2 + a_1 30 + a_0 & \mapsto & x & \mapsto & y \equiv x^7 \,(\mathrm{mod}\, 38009) & \mapsto & y = b_3 30^2 + b_2 30^2 + b_1 30 + b_0 \end{array}$$

Recordemos que para calcular $x^7 \,(\mathrm{mod}\, 38009)$ se hace por cuadrados iterados, utilizando que $7 = 1+2+2^2$ tendremos:

$$x^7 = x \cdot x^2 \cdot x^{2^2} \Longrightarrow \left\{ \begin{array}{l} x_0 \equiv x \,(\mathrm{mod}\, 38009) \\ x_1 \equiv x_0^2 \,(\mathrm{mod}\, 38009) \\ x_2 \equiv x_1^2 \,(\mathrm{mod}\, 38009) \end{array} \right\} \Longrightarrow x^7 \equiv x_0 \cdot x_1 \cdot x_2 \,(\mathrm{mod}\, 38009).$$

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

$$\begin{array}{rl} f(\mathrm{AST}) = & f(18 \cdot 30 + 19) = f(559) \equiv 559^7 \,(\mathrm{mod}\, 38009) \equiv 24608 \,(\mathrm{mod}\, 38009) \Leftrightarrow 24608 = 0 \cdot 30^3 + 27 \cdot 30^2 + 10 \cdot 30 + 8 = \mathrm{A¡KI} \\ f(\mathrm{ANA}) = & f(13 \cdot 30) = f(390) \equiv 390^7 \,(\mathrm{mod}\, 38009) \equiv 29959 \,(\mathrm{mod}\, 38009) \Leftrightarrow 29959 = 1 \cdot 30^3 + 3 \cdot 30^2 + 8 \cdot 30 + 19 = \mathrm{BDIT} \end{array}$$

El mensaje cifrado es **A¡KIBDIT**.

2. Recibimos el texto CFPPC¿MQBX que ha sido encriptado mediante una función de cifrado matricial lineal sobre digrafos. Sabemos que el texto comienza por EL PAIS. Calcular la función de cifrado y descifrar el mensaje completo.

Solución: Sea $f : (\mathbb{Z}/30\mathbb{Z})^2 \longrightarrow (\mathbb{Z}/30\mathbb{Z})^2$ la función de cifrado. Esto es, para $x \in (\mathbb{Z}/30\mathbb{Z})^2$, se define como $f(x) = Ax$, donde $A \in \mathrm{GL}_2(\mathbb{Z}/30\mathbb{Z})$. Sabemos

$$\left. \begin{array}{lll} f(EL) = CF & \Rightarrow & A\binom{4}{11} = \binom{2}{5} \\ f(PA) = PP & \Rightarrow & A\binom{15}{0} = \binom{15}{15} \\ f(IS) = C?\text{`} & \Rightarrow & A\binom{8}{18} = \binom{2}{28} \end{array} \right\} \Rightarrow \begin{array}{l} A\left(\begin{smallmatrix} 4 & 15 \\ 11 & 0 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 2 & 15 \\ 5 & 15 \end{smallmatrix}\right) \Leftrightarrow AP_1 = C_1 \\ A\left(\begin{smallmatrix} 15 & 8 \\ 0 & 18 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 15 & 2 \\ 15 & 28 \end{smallmatrix}\right) \Leftrightarrow AP_2 = C_2 \\ A\left(\begin{smallmatrix} 4 & 8 \\ 11 & 18 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 2 & 2 \\ 5 & 28 \end{smallmatrix}\right) \Leftrightarrow AP_3 = C_3 \end{array}$$

Calculando obtenemos $det(P_1) = 15$, $det(P_2) = 0$ y $det(P_3) = 14$. Como $(det(P_i), 30) \neq 1$ tenemos que P_i no es invertible en $\mathrm{GL}_2(\mathbb{Z}/30\mathbb{Z})$, $i = 1, 2, 3$. Por lo tanto no podemos calcular A directamente a partir de algún par P_i, C_i para ningún $i = 1, 2, 3$. Sin embargo lo que si que tenemos es $(det(P_1), 2) = 1$ y $(det(P_3), 15) = 1$. Por lo tanto podemos calcular $P_1^{-1} \in M_2(\mathbb{Z}/2\mathbb{Z})$ y $P_3^{-1} \in M_2(\mathbb{Z}/15\mathbb{Z})$. Así calculamos $(\overline{P_1})^{-1} \in M_2(\mathbb{Z}/2\mathbb{Z})$ y $(\overline{P_3})^{-1} \in M_2(\mathbb{Z}/15\mathbb{Z})$, donde $\overline{P_1}$ (resp. $\overline{P_3}$) representa P_1 módulo 2 (resp. P_3 módulo 15). Así podemos calcular A módulo 2 y A módulo 15. Y a partir de estas reducciones mediante el teorema chino del resto obtener A ya que $30 = 2 \cdot 15$ y $mcd(2, 15) = 1$:

$$\left.\begin{array}{l} A \equiv C_1(P_1)^{-1} \pmod 2 \equiv \left(\begin{smallmatrix} 0 & 1 \\ 1 & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right) \equiv \left(\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right) \pmod 2 \\ A \equiv C_3(P_3)^{-1} \pmod{15} \equiv \left(\begin{smallmatrix} 2 & 2 \\ 5 & 13 \end{smallmatrix}\right)\left(\begin{smallmatrix} 12 & 8 \\ 11 & 11 \end{smallmatrix}\right) \equiv \left(\begin{smallmatrix} 1 & 8 \\ 8 & 3 \end{smallmatrix}\right) \pmod{15} \end{array}\right\} \overset{TCR}{\Longrightarrow} A = \left(\begin{smallmatrix} 1 & 8 \\ 23 & 3 \end{smallmatrix}\right)$$

Por lo tanto la función de cifrado es

$$f(x, y) = A\left(\begin{smallmatrix} x \\ y \end{smallmatrix}\right) = \left(\begin{smallmatrix} 1 & 8 \\ 23 & 3 \end{smallmatrix}\right)\left(\begin{smallmatrix} x \\ y \end{smallmatrix}\right)$$

y la descifrado es

$$f^{-1}(u, v) = A^{-1}\left(\begin{smallmatrix} u \\ v \end{smallmatrix}\right) = \left(\begin{smallmatrix} 27 & 8 \\ 23 & 29 \end{smallmatrix}\right)\left(\begin{smallmatrix} u \\ v \end{smallmatrix}\right)$$

Por lo tanto para descifrar el resto del mensaje:

$$f^{-1}(MQ) = f^{-1}\left(\begin{smallmatrix} 12 \\ 16 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 2 \\ 20 \end{smallmatrix}\right) = CU \quad ; \quad f^{-1}(BX) = f^{-1}\left(\begin{smallmatrix} 1 \\ 23 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right) = BA$$

Por lo tanto el mensaje descifrado es

EL PAIS CUBA.

3. Calcular $A_{11}(10, 3)$.

Solución: En primer lugar vamos a utilizar algunas de las cotas que conocemos. Recordemos que la cota de Singleton en el caso de $(n, M, d)_q$-códigos dice: $M \leq q^{n-d+1}$. Así en nuestro caso tenemos $M \leq 11^{10-3+1} = 11^8$. Por lo tanto tenemos una primera cota $A_{11}(10, 3) \leq 11^8$. Ahora utilicemos la cota de Hamming. Recordemos que si tenemos un $(n, M, d)_q$-código con $d = 2t + 1$ ó $d = 2t + 2$, este ha de cumplir:

$$M \sum_{i=0}^{t} \left(\begin{smallmatrix} n \\ i \end{smallmatrix}\right) (q-1)^i \leq q^n.$$

En nuestro caso tenemos $M \leq 11^{10}/(1 + 10 \cdot 10) < 256806184 \sim 11^{8,075}$. Así que esta cota es peor que la anterior.

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

$$\sum_{i=0}^{d-2} \left(\begin{smallmatrix} n-1 \\ i \end{smallmatrix}\right) (q-1)^i < q^{n-k},$$

entonces existe un $[n, k, d]_q$-código. En nuestro caso tenemos $1 + 9 \cdot 10 < 11^{10-k}$; que se cumple para $k \leq 8$. Así que en particular tenemos que existe un $[10, 8, 3]_{11}$-código. Este código tendrá 11^8 palabras, que iguala la cota de Singleton en este caso. Por lo tanto $A_{11}(10, 3) = 11^8$

Observar que de hecho sabemos construir este código y que no hubiera sido necesario demostrar su existencia utilizando la cota de Gilbert–Varshamov. Vamos a construir una matriz de paridad H de un $[10, 8, 3]_{11}$-código. Como $n = 10$ y $k = 8$ se tiene que una matriz de paridad será de orden 2x10. Así vamos a imitar la construcción de los códigos de Hamming para construir H. Es decir, queremos construir una matriz con 2 filas y 10 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 $[10, 8, 3]_{11}$-código:

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

4. Un código lineal C se dice autodual si $C = C^{\perp}$. Demostrar

(i) C es un $[2m, m]$-código para algún entero positivo m.

(ii) Toda matriz generadora de C es matriz de paridad y recíprocamente.

(iii) Si $G = (Id_m|A)$ es una matriz generadora de C, entonces $H = (-A^{\top}|Id_m)$ también lo es.

Solución: Supongamos que C es un $[n, k]_q$-código. Sea G una matriz generadora de C, por lo que tendremos $C = \{uG : u \in \mathbb{F}_q^k\}$. Por otro lado si H es una matriz de paridad de C se tiene que es una matriz generadora de su código dual, esto es $C^{\perp} = \{vH : v \in \mathbb{F}_q^{n-k}\}$.
Ahora supongamos $C = C^{\perp}$. Entonces $k = dim(C) = dim(C^{\perp}) = n-k$. Es decir, $n = 2k$. Esto demuestra (i). Además tendremos $C = \{uG : u \in \mathbb{F}_q^k\} = \{vH : u \in \mathbb{F}_q^k\} = C^{\perp}$. Esto nos dice que G es una matriz generadora de $C^{\perp}$ y que H es una matriz generadora de C, demostrando (ii). Por último supongamos que G esta dada en forma estándar: $G = (Id_k|A)$. Por lo tanto la matriz de paridad será de la forma: $H = (-A^{\top}|Id_k)$. Ahora por (ii) tenemos que esta H es una matriz generadora de C.

5. Sea C el código lineal generado por la matriz

$$G = \begin{pmatrix} 0 & 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 2 & 0 & 1 & 0 \\ 0 & 0 & 3 & 0 & 1 & 1 \\ 0 & 1 & 4 & 0 & 1 & 0 \end{pmatrix} \in M_{4x6}(\mathbb{F}_5).$$

(i) Demostrar que es un código Hamming $Ham(r, q)$ y determinar r y q.
(ii) Se ha utilizado el código C para cifrar digrafos escritos en el alfabeto de 25 letras en el que $A = 0$, $B = 1, \ldots, Z = 24$ de la siguiente forma: cada digrafo corresponde a un par $(n, m) \in (\mathbb{Z}/25\mathbb{Z})^2$. Escribimos $n = 5a + b$ y $m = 5c + d$ con $a, b, c, d \in \mathbb{F}_5$. Así cada digrafo corresponde a un vector $(a, b, c, d) \in (\mathbb{F}_5)^4$ y lo codificamos mediante $(a, b, c, d) \cdot G \in (\mathbb{F}_5)^6 = (x_1, x_2, x_3, x_4, x_5, x_6)$. Así convertimos el digrafo definido por el par $(5a+b, 5c+d)$ en el trigrafo que viene dado por $(5x_1 + x_2, 5x_3 + x_4, 5x_5 + x_6)$. Si recibimos el mensaje FSPUSP. Asegúrate qué hemos recibido o que hemos de hacer.

Solución: (i) La matriz $\mathcal{G}$ es equivalente a la siguiente matriz en forma estándar

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

Así construimos la matriz de paridad siguiente

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

Tenemos que las columnas de H son vectores representativos de $\mathbb{P}^1(\mathbb{F}_5)$. Por lo tanto C es el código de Hamming $Ham(2, 5)$.
Otra forma de demostrar (i) es la siguiente: Se observa que la matriz H obtenida anteriormente no tiene ninguna columna formada por ceros, ni ningún par de columnas son proporcionales. Además las primeras cuatro columnas son combinación lineal de la quinta y la sexta. Por lo tanto tenemos que C es un $[6, 4, 3]_3$-código. Además se tiene

$$5^4 \left(\begin{pmatrix} 6 \\ 0 \end{pmatrix} + \begin{pmatrix} 6 \\ 1 \end{pmatrix} (5-1) \right) = 5^6.$$

Esto es, C es un código lineal perfecto con $d = 3$. Por lo tanto es un código Hamming $Ham(r, q)$. Aquí se tiene $q = 5$ y $6 = (5^r - 1)/(5 - 1)$, de lo que se deduce $r = 2$. Así concluimos que C es el código de Hamming $Ham(2, 5)$.

(ii) Recordemos que el método de decodificación por síndromes es un algoritmo que nos permite la decodificiación por mínima distancia para códigos lineales. Además sabemos que si el código tiene distancia $d = 2t + 1$ ó $d = 2t + 2$, entonces si se ha cometido hasta t errores, entonces el código los corrige. Como hemos visto en (i) que la distancia $d = 3$ por ser un código de Hamming tenemos que todos los errores simples los corregirá.

El código utilizado asigna a cada digrafo un trigrafo. Así el mensaje recibido hay que dividirlo en trigrafos, para posteriormente escribirlo como vectores de $\mathbb{F}_5^6$. En nuestro caso:

$$\left.\begin{array}{l} \texttt{F} \leftrightarrow 5 = 1 \cdot 5 + 0 \leftrightarrow (1,0) \\ \texttt{S} \leftrightarrow 18 = 3 \cdot 5 + 3 \leftrightarrow (3,3) \\ \texttt{P} \leftrightarrow 15 = 3 \cdot 5 + 0 \leftrightarrow (3,0) \end{array}\right\} \Leftrightarrow \texttt{FSP} \leftrightarrow (1,0,3,3,3,0)$$

$$\left.\begin{array}{l} \texttt{U} \leftrightarrow 20 = 4 \cdot 5 + 0 \leftrightarrow (4,0) \\ \texttt{S} \leftrightarrow 18 = 3 \cdot 5 + 3 \leftrightarrow (3,3) \\ \texttt{P} \leftrightarrow 15 = 3 \cdot 5 + 0 \leftrightarrow (3,0) \end{array}\right\} \Leftrightarrow \texttt{USP} \leftrightarrow (4,0,3,3,3,0)$$

Hemos visto que C es 1-corrector. Si nos mandan una palabra código $c \in C$ y hemos recibido $x = c + e$, donde $e \in \mathbb{F}_5^6$ es el error, si $\omega(e) \leq 1$ el código C corregirá correctamente. Si $\omega(e) = 0$ esto quiere decir que $c = x \in C$. 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 $x_1 = (1, 0, 3, 3, 3, 0)$ y $x_2 = (4, 0, 3, 3, 3, 0)$. Vamos a decodificar utilizando el método de los síndromes:

$$s_H(x_1) = (1,0,3,3,3,0)H^t = (3,4) = 1 \cdot {H_1}^t \quad \Longrightarrow \quad c_1 = x_1 - 1 \cdot e_1 \quad \Longrightarrow \quad c_1 = (0,0,3,3,3,0)\,,$$

$$s_H(x_2) = (4,0,3,3,3,0)H^t = (2,1) = -1 \cdot {H_1}^t \quad \Longrightarrow \quad c_2 = x_2 + 1 \cdot e_1 \quad \Longrightarrow \quad c_2 = (0,0,3,3,3,0)\,.$$

Las palabra del código C son de la forma $(a, b, c, d)G = (b, d, a + 2b + 3c + 4d, a, a + b + c + d, c)$ donde $a, b, c, d \in \mathbb{F}_5$, entonces en nuestro caso obtenemos:

$$c_1 = c_2 = (0,0,3,3,3,0) \Longrightarrow (3,0,0,0) \Longrightarrow n = 5 \cdot 3 + 0 = 15,\ m = 5 \cdot 0 + 0 = 0 \Longrightarrow \texttt{PA}$$

Por lo tanto la palabra enviada es:

$$\texttt{PAPA}\,.$$