TEORÍA DE CÓDIGOS Y CRIPTOGRAFÍA | **Examen 25-11-2011**

SOLUCIONES

El alfabeto utilizado en todos los ejercicios 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. Interceptamos un mensaje de Marcos que dice

$$ZQXSMOTIGQ$$

Sabemos que Marcos siempre firma sus mensajes y que en este caso ha cifrado el mensaje utilizando un cifrado matricial lineal sobre digrafos. Descifrar el mensaje.

Solución: Sea $f : (\mathbb{Z}/26\mathbb{Z})^2 \longrightarrow (\mathbb{Z}/26\mathbb{Z})^2$ la función de cifrado. Esto es, para $x \in (\mathbb{Z}/26\mathbb{Z})^2$, se define como $f(x) = Ax$, donde $A \in \mathrm{GL}_2(\mathbb{Z}/26\mathbb{Z})$. Sabemos

$$\left.\begin{array}{lcl} f(MA) = MO & \Rightarrow & A\binom{12}{0} = \binom{12}{14} \\ f(RC) = TI & \Rightarrow & A\binom{17}{2} = \binom{19}{8} \\ f(OS) = GQ & \Rightarrow & A\binom{14}{18} = \binom{6}{16} \end{array}\right\} \Rightarrow \begin{array}{l} A\left(\begin{smallmatrix} 12 & 17 \\ 0 & 2 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 12 & 19 \\ 14 & 8 \end{smallmatrix}\right) \Leftrightarrow AP_1 = C_1 \\ A\left(\begin{smallmatrix} 17 & 14 \\ 2 & 18 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 19 & 6 \\ 8 & 16 \end{smallmatrix}\right) \Leftrightarrow AP_2 = C_2 \\ A\left(\begin{smallmatrix} 12 & 14 \\ 0 & 18 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 12 & 6 \\ 14 & 16 \end{smallmatrix}\right) \Leftrightarrow AP_3 = C_3 \end{array}$$

Calculando obtenemos $det(P_1) = 24$, $det(P_2) = 18$ y $det(P_3) = 8$. Como $(det(P_i), 26) \neq 1$ tenemos que P_i no es invertible en $\mathrm{GL}_2(\mathbb{Z}/26\mathbb{Z})$, $i = 1, 2, 3$. Sin embargo, si lo van a ser en $\mathrm{GL}_2(\mathbb{Z}/13\mathbb{Z})$ ya que $(det(P_i), 13) \neq 1$.
Vamos a trabajar con $i = 1$. Así obtenemos $A \equiv C_1 \cdot P_1^{-1} (\mathrm{mod}\ 13)$. Es decir, $A \equiv \left(\begin{smallmatrix} 1 & 1 \\ 12 & 6 \end{smallmatrix}\right) (\mathrm{mod}\ 13)$. De lo que deducimos:

$$A = \left(\begin{smallmatrix} 1 & 1 \\ 12 & 6 \end{smallmatrix}\right) + 13B, \qquad \text{donde} \quad B = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right), \quad a, b, c, d \in \{0, 1\}.$$

Ahora, sabemos que $A \in \mathrm{GL}_2(\mathbb{Z}/26\mathbb{Z})$, por lo tanto A será también invertible módulo 2. Si denotamos por $\overline{A}$ la reducción de A módulo 2 obtenemos que

$$\overline{A} \in \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z}) = \left\{ \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & 1 \\ 1 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 1 \\ 1 & 0 \end{smallmatrix}\right) \right\}.$$

Como B es igual a B módulo 2, reducimos módulo 2 la ecuación anterior y obtenemos

$$B = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 0 \end{smallmatrix}\right) + \overline{A}\,.$$

Ahora utilizando las 6 posibles formas que puede tener $\overline{A}$ y obtenemos 6 posibles B's:

$$B \in \left\{ \left(\begin{smallmatrix} 0 & 1 \\ 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 0 \\ 1 & 0 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & 1 \\ 1 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & 0 \\ 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & 0 \\ 1 & 0 \end{smallmatrix}\right) \right\},$$

y de aquí las 6 posibles A's: $\left(\begin{smallmatrix} 1 & 14 \\ 12 & 19 \end{smallmatrix}\right), \left(\begin{smallmatrix} 14 & 1 \\ 25 & 6 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 14 \\ 25 & 19 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 1 \\ 12 & 19 \end{smallmatrix}\right), \left(\begin{smallmatrix} 14 & 1 \\ 25 & 19 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 1 \\ 25 & 6 \end{smallmatrix}\right)$. Ahora imponemos las condiciones $AP_i = C_i$, $i = 1, 2, 3$. Entonces sólo dos matrices pasan esta criba:

$$A_1 = \left(\begin{smallmatrix} 1 & 14 \\ 12 & 19 \end{smallmatrix}\right) \qquad \text{y} \qquad A_2 = \left(\begin{smallmatrix} 1 & 1 \\ 12 & 19 \end{smallmatrix}\right).$$

Por lo tanto las posibles funciones de cifrado son de la forma $f_i(x) = A_i \cdot x$ para $i = 1, 2$. Veamos cuál es la correcta. Aplicando f_i^{-1} a ZQXS obtenemos:

$$f_i^{-1}(ZQ) = f_i^{-1}\binom{25}{16} = \binom{21}{4} = VE \quad ; \quad f_i^{-1}(XS) = f_i^{-1}\binom{23}{18} = \binom{19}{4} = TE$$

para ambas funciones. Por lo tanto ambas son solución y el mensaje es

$$VETEMARCOS.$$

2. Factorizar 2599 utilizando el método de Kraitchick–Dixon.

Solución: Sea n un entero compuesto. El método de Kraitchick–Dixon consiste en primer lugar en tomar el polinomio $Q(x) = x^2 \pmod n$ y una base de primos $\mathcal{B}$. Luego se toma un conjunto finito S de enteros tales que para todo $i \in S$ los enteros $c_i = Q(\lfloor\sqrt{n}\rfloor + i)$ son producto de potencias de primos perteneciente a la base $\mathcal{B}$. Por último se busca un subconjunto $S_0 \subseteq S$ tal que

$$\prod_{i \in S_0} c_i = \alpha^2, \qquad \text{para algún } \alpha \in \mathbb{Z}.$$

Entonces si denotamos por $\beta = \prod_{i \in S_0} (\lfloor\sqrt{n}\rfloor + i)$ tenemos que $\alpha^2 \equiv \beta^2 \pmod{\text{n}}$. De aqui obtenemos $d_\pm = mcd(\alpha \pm \beta, n)$ es un divisor de n. El algoritmo concluye si $d_\pm \neq 1, n$. En caso contrario, se tiene que cambiar alguno de los conjuntos $\mathcal{B}, S$ o/y S_0.
Ahora vamos a aplicar este método a nuestro entero $n = 2599$. En primer lugar calculamos $\lfloor\sqrt{n}\rfloor = 50$ y vamos a tomar $\mathcal{B} = \{2, 3, 5, 7\}$. Los primeros valores de c_i son

$$c_1 = 2, \qquad c_2 = 3 \cdot 5 \cdot 7, \qquad c_3 = 2 \cdot 3 \cdot 5 \cdot 7.$$

Así tenemos $c_1 c_2 c_3 = (2 \cdot 3 \cdot 5 \cdot 7)^2$. Por lo tanto tenemos $(51 \cdot 52 \cdot 53)^2 \equiv (2 \cdot 3 \cdot 5 \cdot 7)^2 \pmod{2599}$. Ahora calculamos

$$mcd(n, 51 \cdot 52 \cdot 53 - 2 \cdot 3 \cdot 5 \cdot 7) = n \qquad \text{y} \qquad mcd(n, 51 \cdot 52 \cdot 53 + 2 \cdot 3 \cdot 5 \cdot 7) = 1.$$

Por lo tanto, el algoritmo con los conjuntos que hemos tomado no nos da una solución. Vamos a calcular más valores de c_i. El siguiente i que cumple que sus factores son potencias de primos pertenecientes a $\mathcal{B}$ es $i = 9$. En ese caso tenemos $c_9 = 2 \cdot 3^2 \cdot 7^2$. Vemos que $c_1 c_9 = (2 \cdot 3 \cdot 7)^2$. Entonces intentamos con $S_0 = \{1, 9\}$:

$$mcd(n, 51 \cdot 59 - 2 \cdot 3 \cdot 7) = 23 \qquad \text{y} \qquad mcd(n, 51 \cdot 59 + 2 \cdot 3 \cdot 7) = 113.$$

Así vemos que $2599 = 23 \cdot 113$. Para concluir el ejercicio nos queda ver que los factores 23 y 113 son primos. Vamos a utilizar que si m es entero compuesto entonces existe un divisor primo p menor que $\sqrt{m}$. En nuestro caso para ver que 23 es primo es suficiente con ver que no es divisible ni por 2 ni por 3 y en el caso 113 para los primos $2, 3, 5$ ni 7.

3. La clave pública RSA de Alberto es $(n, e) = (2599, 2085)$. Alguien le ha enviado el siguiente mensaje:

CDYADB

¿Qué le han querido decir?

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. Podemos utilizar el ejercicio 2 o bien factorizar n de otra forma. En primer lugar hagámoslo mediante fuerza bruta. Esto es, vamos a utilizar que n siempre tiene un divisor primo p menor que $\sqrt{n} < 50$. Por lo tanto dividiendo por los primeros primos: $2, 3, 5, 7, 11, 13, 17, 19, 23$ observamos que podemos parar en 23, ya que divide a n. El otro divisor es 113. Además como nos aseguran que n es un módulo RSA sabemos que es el producto de dos primos. Otra forma es el Método de Fermat. Sea $Q(x) = x^2 - n = x^2 - 2599$. 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 $i = 18$ tenemos $Q(68) = 3^4 5^2$. Por lo tanto los divisores de n son $68 + 3^2 5 = 113$ y $68 - 3^2 5 = 23$.
Así hemos calculado $\varphi(n) = 2464$, 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 $d = 13$. Ya tenemos la clave de descifrado.

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

$$l_1 = \left\lfloor \frac{\log 2599}{\log 26} \right\rfloor = 2 \qquad \text{y} \qquad l_2 = \left\lceil \frac{\log 2599}{\log 26} \right\rceil = 3.$$

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

$$\begin{array}{ccccccc} \mathbb{Z}/26^2\mathbb{Z} & \hookrightarrow & \mathbb{Z}/2599\mathbb{Z} & \xrightarrow{f} & \mathbb{Z}/2599\mathbb{Z} & \hookrightarrow & \mathbb{Z}/26^3\mathbb{Z} \\ x = a_1 26 + a_0 & \mapsto & x & \mapsto & y \equiv x^{2085} \,(\mathrm{mod}\, 2599) & \mapsto & y = b_2 26^2 + b_1 26 + b_0 \end{array}$$

De forma equivalente la inversa:

$$\begin{array}{ccccccc} \mathbb{Z}/26^3\mathbb{Z} & \to & \mathbb{Z}/2599\mathbb{Z} & \xrightarrow{f^{-1}} & \mathbb{Z}/2599\mathbb{Z} & \to & \mathbb{Z}/26^3\mathbb{Z} \\ y = b_2 26^2 + b_1 26 + b_0 & \mapsto & y & \mapsto & x \equiv y^{13} \,(\mathrm{mod}\, 2599) & \mapsto & x = a_1 26 + a_0 \end{array}$$

Recordemos que para calcular $y^{13} \,(\mathrm{mod}\, 2599)$ se hace por cuadrados iterados, utilizando que $13 = 1 + 2^2 + 2^3$ tendremos:

$$y^{13} = y \cdot y^{2^2} \cdot y^{2^3} \Longrightarrow \left\{ \begin{array}{l} y_0 \equiv y \,(\mathrm{mod}\, 2599) \\ y_1 \equiv y_0^2 \,(\mathrm{mod}\, 2599) \\ y_2 \equiv y_1^2 \,(\mathrm{mod}\, 2599) \\ y_3 \equiv y_2^2 \,(\mathrm{mod}\, 2599) \end{array} \right\} \;,\; \left\{ \; w_0 = y_0 \cdot y_2 \,(\mathrm{mod}\, 2599) \; \right\} \Longrightarrow y^{13} \equiv w_0 \cdot y_3 \,(\mathrm{mod}\, 2599).$$

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

$$\begin{array}{lrl} f^{-1}(\mathrm{CDY}) = & f^{-1}(2 \cdot 26^2 + 3 \cdot 26 + 24) = f^{-1}(1454) \equiv 1454^{13} \,(\mathrm{mod}\, 2599) \equiv 550 \,(\mathrm{mod}\, 2599) \Leftrightarrow 550 = 21 \cdot 26 + 4 & = \mathrm{VE} \\ f^{-1}(\mathrm{ADB}) = & f^{-1}(0 \cdot 26^2 + 3 \cdot 26 + 1) = f^{-1}(79) \equiv 79^{13} \,(\mathrm{mod}\, 2599) \equiv 498 \,(\mathrm{mod}\, 2599) \Leftrightarrow 498 = 19 \cdot 26 + 4 & = \mathrm{TE} \end{array}$$

El mensaje descifrado es VETE.

4. Demostrar que hay infinitos pseudoprimos en base 2.
Ayuda:

(i) ¿Es 341 un pseudoprimo en base 2?

(ii) Demostrar que si n es pseudoprimo en base 2 entonces $2^n - 1$ también es pseudoprimo en base 2.

Solución: Recordemos que un entero compuesto n es pseudoprimo en base b si $b^{n-1} \equiv 1 \,(\mathrm{mod}\ n)$. Veamos en primer lugar que 341 es pseudoprimo en base 2. Factorizando vemos que $341 = 11 \cdot 31$. Ahora que $2^{340} \equiv 1 \,(\mathrm{mod}\ 341)$. Para ello vamos a utilizar cuadrado iterados: $340 = 2^2 + 2^4 + 2^6 + 2^8$. Así obtenemos

k	1	2	3	4	5	6	7	8
$2^{2^k} \,(\mathrm{mod}\ 341)$	4	16	256	64	4	16	256	64

por lo tanto como $16 \cdot 64 \equiv 1 \,(\mathrm{mod}\ 341)$, obtenemos $2^{340} \equiv 1 \,(\mathrm{mod}\ 341)$.
Ahora demostremos (ii): necesitamos ver que $2^{m-1} \equiv 1 \,(\mathrm{mod}\ m)$ donde $m = 2^n - 1$. Es decir, $2^n - 1$ divide a $2^{m-1} - 1$, o equivalentemente, n divide a $m - 1 = 2^n - 1 - 1 = 2^n - 2 = 2(2^{n-1} - 1)$. Como $n \neq 2$, tenemos que esto es equivalente a que n divida a $2^{n-1} - 1$, esto es, $2^{n-1} \equiv 1 \,(\mathrm{mod}\ n)$. O lo que es lo mismo, que n sea pseudoprimo en base 2.
Una vez que hemos visto en (i) que 341 es pseudoprimo en base 2 podemos hacer una construcción iterativa utilizando (ii) para obtener infinitos pseudoprimos en base 2.