MA-53G Intr. a la Criptografía **Semestre Primavera, 1996**

Cátedra No. 9 : 3 de Septiembre

Transcriptor: Marcos Kiwi[1]

1 Pendientes

Uno de los puntos pendientes que nos quedaba verificar acerca de RSA era que la función de decripción correspondía a la función inversa de la función de encripción. Primero recordemos que en el criptosistema de RSA se tiene que $\mathcal{P} = \mathcal{C} = \mathcal{Z}_n$, donde $n = pq$ (p y q primos). Además, en RSA el conjunto de claves es $\mathcal{K} = \{(p,q,e,d) \mid n = pq,\ ed \equiv 1 \pmod{\varphi(n)}\}$, donde $\varphi(n)$ es la función de Euler. Para $K = (p,q,e,d) \in \mathcal{K}$ se tiene que las reglas de encripción y decripción vienen dadas respectivamente por

$$\begin{aligned} e_k(x) &= x^e \bmod n\,, \qquad \forall x \in \mathcal{P}\,, \\ d_k(y) &= y^d \bmod n\,, \qquad \forall y \in \mathcal{C}\,. \end{aligned}$$

Finalmente recordemos que la parte pública de la clave era la tupla (n,e).

Queremos verificar que cualquiera sea el texto plano x y la clave $k = (p,q,e,d) \in \mathcal{K}$ se tiene que $d_k(e_k(x)) = x$. Para ello notar que existe un entero t tal que $ed = t\varphi(n)+1$. Luego, si x es primo relativo con n, entonces

$$x^{ed} \equiv x^{t\varphi(n)+1} \equiv (x^{\varphi(n)})^t x \equiv x \pmod{n}\,.$$

Donde la última congruencia se deduce del Teorema de Euler. Por otro lado, si x no es primo relativo con n, suponemos sin perdida de generalidad que x no es primo relativo con p y que es primo relativo con q (si $x \in \mathcal{P} = \mathcal{Z}_n$ entonces x debe ser primo relativo con p o con q). Luego,

$$\begin{aligned} x^{ed} &\equiv x &&\equiv 0 \pmod{p}\,, \\ x^{ed} &\equiv (x^{q-1})^{t(p-1)}x &&\equiv x \pmod{q}\,. \end{aligned}$$

Donde la segunda congruencia es consecuencia del pequeño Teorema de Fermat y puesto que si $n = pq$ entonces $\varphi(n) = (p-1)(q-1)$. Luego, tanto x como x^{ed} son soluciones del mismo sistema de congruencias. Pero como p y q son primos relativos, el Teorema Chino del Resto permite concluir que x^{ed} y x son congruentes módulo n, i.e. $x^{ed} \equiv x \pmod{n}$. En otras palabras, $d_k(e_k(x)) = x$ como queriamos demostrar.

[1] Basada en una transcripción parcial por Francisco Valdés

2 Más Teoría de Números (Continuación)

Ahora que hemos retomado nuestro estudio de Teoría de Números aprovechamos para probar un resultado que habiamos mencionado antes y que concierne a la función φ de Euler.

Lema 1 *La función φ de Euler es multiplicativa, i.e. si m y n son primos relativos*

$$\varphi(mn) \;=\; \varphi(m)\varphi(n)\,.$$

Dem: La idea de la demostración es identificar cada elemento de $\mathcal{Z}^*_{mn}$ con un único elemento de $\mathcal{Z}^*_m \times \mathcal{Z}^*_n$. Sea $j \in \{1, \ldots, mn\}$ y sean $j_1 = j \bmod n$, $j_2 = j \bmod m$. Notar que j_1 es primo relativo con n si y sólo si j es primo relativo con n. Analogamente, j_2 es primo relativo con n si y sólo si j es primo relativo con n. Luego, por el Teorema Chino del Resto, los $j \in \{1, \ldots, mn\}$ que son primos relativos a mn se pueden asociar 1 a 1 con los pares (j_1, j_2) tales que $j_1 \in \{1, .., n\}$, $j_2 \in \{1, .., m\}$, j_1 es primo relativo con n, y j_2 es primo relativo con m. Sigue que, $\varphi(mn) = \varphi(m)\varphi(n)$. $\square$

Lema 2 *Para todo n entero positivo, se tiene que $\displaystyle\sum_{d|n} \varphi(d) = n$.*

Dem: Sea $f(n) = \sum_{d|n} \varphi(d)$. Se quiere probar que $f(n) = n$. Notar que la afirmación es evidente si n es primo, pues en este caso $f(n) = \varphi(1) + \varphi(n) = 1 + (n-1)$. Más aun, si $n = p^k$ donde p es primo,

$$f(p^k) \;=\; \sum_{i=0}^{k} \varphi(p^i) \;=\; 1 + \sum_{i=1}^{k} (p^i - p^{i-1}) \;=\; p^k\,.$$

Luego, para concluir que $f(n) = n$ con n arbitrario, bastará aplicar el Teorema Fundamental de la Aritmética y probar que f es una función multiplicativa, i.e. $f(mn) = f(m)f(n)$ si m y n son primos relativos. Sean entonces m y n primos relativos y d un divisor de mn, entonces existen d_1 y d_2 primos relativos (univocamente determinados) tales que $d = d_1 d_2$, $d_1|m$, $d_2|n$. Luego

$$f(mn) \;=\; \sum_{d|mn} \varphi(d) \;=\; \sum_{d_1|m} \sum_{d_2|n} \varphi(d_1 d_2) \;=\; \sum_{d_1|m} \varphi(d_1) \sum_{d_2|n} \varphi(d_2) \;=\; f(m)f(n)\,.$$

$\square$

3 Cuerpos finitos

Un cuerpo es un conjunto, dotado de dos operaciones; adición y multiplicación. Ambas operaciones son asociativas y conmutativas, hay un elemento neutro para la adición, 0, y un elemento neutro para la multiplicación, 1, todo elemento tiene inverso aditivo y todo elemento distinto de 0 tiene inverso multiplicativo, y la multiplicación distribuye con respecto a la adición. Un cuerpo F se denomina cuerpo finito si $|F|$ es finito. Si sumando la identidad reiterativamente nunca obtenemos el neutro aditivo el cuerpo se dice de característica 0 (e.g. el cuerpo de los números reales).

Para un entero no-negativo q denotaremos por F_q el cuerpo con q elementos. Sea 1 el neutro multiplicativo en F_q, y sea p el menor entero positivo tal que

$$\underbrace{1+1+1+\ldots+1}_{p\ veces} \;=\; 0\,.$$

Dicho entero p existe pues necesariamente debe ocurrir que como F_q tiene cardinalidad finita entonces existen dos enteros $i > j$ tales que

$$\underbrace{1+1+1+\ldots+1}_{i\ veces} \;=\; \underbrace{1+1+1+\ldots+1}_{j\ veces}\,.$$

Luego, p es a lo más $i-j$. Por otro lado, es importante notar que p es necesariamente primo, pues si $p = kl$ para k y l enteros entonces

$$0 \;=\; \underbrace{1+\ldots+1}_{p} \;=\; \underbrace{(1+\ldots+1)}_{k}\underbrace{(1+\ldots+1)}_{l}\,.$$

Como F_q es un cuerpo, no tiene divisores del cero, luego o k o l deben ser iguales a la unidad, i.e. p es primo. A p se le denomina la característica de F_q. Si F_q es de característica p entonces contiene un cuerpo F_p isomorfo a $\mathcal{Z}_p$, denominado cuerpo primo. En efecto

$$F_p \;=\; \{0, 1, 1+1, .., \underbrace{1+..+1}_{(p-1)\ veces}\}\,,$$

dotado de las operaciones adición y multiplicación heredadas de F_q es un cuerpo isomorfo a $\mathcal{Z}_p$.

Ahora probaremos la importante afirmación que dice que que si F_q tiene característica p entonces q debe ser una potencia de p. Observemos antes que F_q es un espacio vectorial sobre F_p, i.e. las operaciones $+\colon\ F_q \times F_q \to F_q$, $\cdot\colon\ F_p \times F_q \to F_q$, satisfacen

1. $(F_q, +)$ es un grupo abeliano.
2. Cualquiera sean los escalares $\alpha, \beta \in F_p$, y los elementos $x, y \in F_q$ se tiene que
   (a) $\alpha(x+y) = \alpha x + \alpha y$.
   (b) $(\alpha\beta)x = \alpha(\beta x)$.
   (c) $(\alpha+\beta)x = \alpha x + \beta x$.
   (d) $1 \cdot x = x$.

Luego, como F_q es un conjunto finito sigue que F_q (visto como espacio vectorial) tiene dimensión finita k. Tomando una base de tamaño k de F_q es fácil establecer una biyección entre F_q y $\{(\lambda_1, \ldots, \lambda_k) \mid \lambda_i \in F_p\}$. De lo anterior se concluye que $q = |F_q| = p^k$. Por lo tanto se puede concluir que sólo existen cuerpos finitos cuya cardinalidad es una potencia de un número primo p.[2]

[2] Aunque no lo probaremos cabe destacar que existe un único cuerpo (salvo isomorfismos) de cardinalidad q.