MA-53G Intr. a la Criptografía **Semestre Otoño, 1998**

Cátedra No. 12 : 28 de Abril

Transcriptor: Gonzalo Navarro[1]

1 Correctitud de RSA

Demostraremos que el esquema de RSA es correcto, es decir que la función de decripción es la inversa de la de encripción. Recordemos que en el criptosistema de RSA se tiene que el conjunto de claves es $\mathcal{K} = \{(n, e, d) \mid n = pq$ donde p y q son primos, $e, d \in \mathcal{Z}_{\varphi(n)}$ y $ed \equiv 1 \pmod{\varphi(n)}\}$, donde $\varphi(n)$ es la función de Euler. Para $K = (n, e, d) \in \mathcal{K}$ se tiene que las reglas de encripción y decripción vienen dadas respectivamente por

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

Finalmente recordemos que la parte pública de la clave es la tupla (n, e) y la parte privada es d.

Queremos verificar que cualquiera sea el texto plano x y la clave $k = (n, e, d) \in \mathcal{K}$ se tiene que $d_k(e_k(x)) = x$. Para ello notar que, como $ed \equiv 1 \pmod{\varphi(n)}\}$, existe un entero t tal que $ed = t\varphi(n) + 1$. Tenemos dos casos

i) $(x, n) = 1$, es decir x es primo relativo con n.

En este caso

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

Donde la última congruencia se deduce del Teorema de Euler, que establece que $x^{\varphi(n)} \equiv 1 \pmod{n}$ siempre que $(x, n) = 1$.

ii) $(x, n) \neq 1$, es decir x *no* es primo relativo con n.

Consideremos el caso $x \neq 0$ (pues si $x = 0$ trivialmente se tiene que $x^{ed} = x$). Dado que x comparte un divisor con $n = pq$, entonces ese divisor debe ser o bien p o bien q. No pueden ser ambos porque al ser p y q primos tendríamos $pq|x$, de donde $x \geq pq = n$, lo cual contradice la suposición de que $0 \leq x < n$ (es decir, $x \in \mathcal{Z}_n$).

Supongamos entonces que $p|x$ y $q \not| x$ (el caso recíproco es análogo). En ese caso $x \equiv 0 \pmod{p}$, de lo cual se deduce $x^{ed} \equiv 0 \equiv x \pmod{p}$. Por otro lado, como $ed \equiv 1 \pmod{\varphi(n)}$, tenemos que para algún entero t, $ed = 1 + t\varphi(n)$. Dado que $n = pq$, $\varphi(n) = (p-1)(q-1)$, y por lo tanto $ed = 1 + t(p-1)(q-1)$. De lo anterior se deduce

$$x^{ed} \equiv (x^{q-1})^{t(p-1)} x \equiv x \pmod{q}\,,$$

[1] La primera parte modificando a Marcos Kiwi.

donde la última congruencia es consecuencia del pequeño Teorema de Fermat, que indica que $x^{q-1} \equiv 1 \pmod{q}$ si q es primo.

Luego, tanto x como x^{ed} son congruentes módulo p y módulo q. Dado que p y q son primos relativos, el Teorema Chino del Resto permite concluir que x^{ed} y x son congruentes módulo $pq = n$, i.e. $x^{ed} \equiv x \pmod{n}$.

En otras palabras, $d_k(e_k(x)) = x$ como queríamos demostrar.

2 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 (denotado 0), y un elemento neutro para la multiplicación (denotado 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 no tiene *divisores de cero*. Esto significa que no existen $a, b \neq 0$ tal que $ab = 0$. Si tal cosa ocurriera, dado que $a \neq 0$ y por ende existe su inverso multiplicativo a^{-1}, multiplicando ambos lados por a^{-1}, obtendríamos $b = 0$, lo que contradice la hipótesis.

Un cuerpo F se denomina cuerpo finito si $|F|$ es finito. Para un entero no-negativo q denotaremos por F_q un cuerpo con q elementos (no lo probaremos, pero todos los cuerpos del mismo cardinal finito son isomorfos).

2.1 Característica de un Cuerpo

Se define la *característica* de un cuerpo como el número de veces que hay que sumar 1 (a partir de 0) para volver a obtener 0. Si sumando 1 reiterativamente nunca obtenemos el 0 se dice que el cuerpo tiene característica 0 (e.g. el cuerpo de los números reales).

Veamos que todo cuerpo finito tiene característica distinta de 0. Sea 1 el neutro multiplicativo en F_q, y sea p el menor entero positivo tal que

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

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

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

Pero como por asociatividad de $+$ vale

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

sumando a ambos lados de la ecuación (1) el inverso aditivo de

$$\underbrace{1+1+1+\ldots+1}_{j\ veces}$$

tendremos

$$\underbrace{1+1+1+\ldots+1}_{i-j\ veces} \quad = \quad 0\,.$$

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 y menores que p entonces por distributividad del producto tenemos

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

Como F_q es un cuerpo, no tiene divisores del cero (es decir, si dos elementos multiplicados dan cero es porque al menos uno de ellos es cero), luego uno de los dos factores debe ser cero, con lo cual ó k ó l deben ser p, o mayores que p (pues p era el menor valor que retornaba a cero), o cero, con lo cual $p=0$. Todas las alternativas son inconsistentes con las hipótesis. Por lo tanto p, la característica de F_q, es siempre primo.

2.2 Cardinalidad de los Cuerpos Finitos

Si F_q es de característica p entonces contiene un cuerpo F_p isomorfo a $\mathcal{Z}_p$, denominado *cuerpo primo*. En efecto

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

dotado de las operaciones adición y multiplicación heredadas de F_q es un cuerpo isomorfo a $\mathcal{Z}_p$. El isomorfismo es el obvio: $1+1+...+1$ (i veces) se mapea a $i\,(\mathrm{mod}\,p)$ [2].

Ahora probaremos la importante afirmación que dice que que si F_q tiene característica p entonces q debe ser una potencia de p.

Para ello, veremos a F_q como un *espacio vectorial*. La idea es considerar a cada elemento de F_q como un vector. El cuerpo escalar sobre el cual se construye este espacio vectorial es F_p. Es decir, aunque F_p pueda ser un subconjunto de F_q, artificialmente consideraremos los elementos de F_p como escalares y los de F_q como vectores. Las operaciones de este espacio vectorial son heredadas del cuerpo F_q, es decir tenemos $+$: $F_q \times F_q \to F_q$, y $\cdot$: $F_p \times F_q \to F_q$ (este último es el producto por "escalar", que definimos como el producto del cuerpo). Las operaciones así definidas satisfacen

1. $(F_q, +)$ es un grupo abeliano (trivial porque $(F_q, +, \cdot)$ es un cuerpo).
2. Cualquiera sean los escalares $\alpha, \beta \in F_p$, y los elementos $x, y \in F_q$ se tiene que

[2] Este isomorfismo muestra, de paso, que dos cuerpos de cardinalidad prima son isomorfos.

(a) $\alpha(x + y) = \alpha x + \alpha y$ (válido porque el producto del cuerpo distribuye con la suma del cuerpo).

(b) $(\alpha\beta)x = \alpha(\beta x)$ (válido porque el producto del cuerpo es asociativo).

(c) $(\alpha + \beta)x = \alpha x + \beta x$ (nuevamente por la distributiva).

(d) $1 \cdot x = x$ (pues 1 es el neutro multiplicativo del cuerpo).

Luego, como F_q es un conjunto finito sigue que F_q (visto como espacio vectorial) tiene dimensión finita k. Recordemos que eso significa que existen k vectores (una "base") tal que todo elemento del espacio vectorial se expresa en forma única como combinación lineal de los vectores de la base. Tomando una base de tamaño k de F_q es fácil establecer una biyección entre F_q y $\{(\lambda_1, \ldots, \lambda_k) \mid \lambda_i \in F_p\}$ (pues cada elemento se identifica con los coeficientes que asigna a los vectores de la base). De lo anterior se concluye que $q = |F_q| = p^k$ (cantidad de combinaciones posibles de valores de escalares). Por lo tanto se puede concluir que sólo existen cuerpos finitos cuya cardinalidad es una potencia de un número primo p.

2.3 Existencia de Cuerpos de Determinada Cardinalidad

Demostraremos ahora la propiedad recíproca a la anterior, es decir, que dado un $q = p^n$, con p primo y $n \in \mathcal{N} - \{0\}$, existe un cuerpo de cardinalidad q.

Si $n = 1$, tenemos que $q = p$, es decir q mismo es primo. En este caso sabemos inmediatamente que existen cuerpos de cardinalidad q, puesto que $(\mathcal{Z}_q, +, \cdot)$ es un cuerpo para q primo.

De modo que nos interesará el caso $n > 1$, es decir cuando q no es primo. Los cuerpos de cardinal primo se llaman "primales", de modo que nos interesan los no primales.

Si $\mathcal{K}$ es un cuerpo, llamaremos $\mathcal{K}[X]$ al anillo de polinomios en la indeterminada X y con coeficientes en $\mathcal{K}$. Formalmente,

$$\mathcal{K}[X] \;=\; \bigcup_{n \in \mathcal{N}} \left\{ \sum_{i=0}^{n} c_i \; X^i \; ; \; c_i \in \mathcal{K} \right\} .$$

Es importante entender que las sumas y productos que aparecen en la fórmula anterior son formales, es decir nunca se opera realmente. Si se desea se puede pensar al polinomio como una n-tupla de elementos de $\mathcal{K}$. La utilidad de verlos como polinomios es que facilita la definición de la suma y producto en $\mathcal{K}[X]$: son simplemente la suma y producto de polinomios (si se quiere pensar como n-tupla, la suma se realiza término a término y el producto se puede expresar con convoluciones).

Recordemos que un anillo $(R, +, \cdot)$ significa que $(R, +)$ es un grupo abeliano, $\cdot$ es asociativa y distribuye con la suma. Si además existe un neutro multiplicativo 1, se dice que R es un anillo con unidad. Si el producto es conmutativo se dice que R es un anillo conmutativo. Por último, si R es un anillo conmutativo sin divisores del cero (es decir, ningún producto de elementos distintos de cero da cero), se dice que R es un "dominio de integridad". Los polinomios sobre un cuerpo $\mathcal{K}$ forman un dominio de integridad, con unidad.

El siguiente teorema nos muestra, en particular, que utilizando polinomios sobre el cuerpo finito $\mathcal{Z}_p$, y definiendo las operaciones de forma adecuada, se puede construír un cuerpo de cardinalidad p^n.

Teorema: Sea $\mathcal{K}$ un cuerpo finito y sea $f \in \mathcal{K}[X]$ un polinomio irreductible[3] de grado n. Entonces $\mathcal{K}[X]/(f)$ [4] es un cuerpo finito con $|\mathcal{K}|^n$ elementos.

Demostración:

Veamos primero cuántos elementos tiene $\mathcal{K}[X]/(f)$. Dado que todos los polinomios son de grado menor que n, todos se pueden escribir de la forma

$$a_0 + a_1 x + a_2 x^2 + ... + a_{n-1} x^{n-1}$$

donde los polinomios de menor grado se obtienen haciendo algunos $a_i = 0$. Está claro que el número de valores posibles para los coeficientes a_i es $|\mathcal{K}|^n$. Por otro lado, todo polinomio de grado menor que n es irreductible módulo f, de forma que el cardinal de $\mathcal{K}[X]/(f)$ es exactamente $|\mathcal{K}|^n$ (observar que se trata de un conjunto finito).

Veamos ahora que $\mathcal{K}[X]/(f)$ es un dominio de integridad. La conmutatividad del producto se hereda obviamente de la de $\mathcal{K}$. Para ver que no hay divisores de cero, sean $g, h \in \mathcal{K}[X]/(f)$ que cumplen $gh = 0 \in \mathcal{K}[X]/(f)$. Por la definición de este anillo esto significa que $f|gh$, es decir existe un polinomio p tal que $gh = pf$. Al ser f irreductible, esto implica que $f|g$ ó $f|h$, es decir g ó h son congruentes con cero módulo f, o sea son cero en el anillo $\mathcal{K}[X]/(f)$.

Veamos por último que todo dominio de integridad finito es un cuerpo. Lo que falta demostrar es que existe el neutro y los inversos multiplicativos. Para ello, consideremos un elemento fijo $x \neq 0$, y definamos la función $f_x(y) = xy$. Esa función debe ser una inyección en $\mathcal{K} - \{0\}$, porque si no lo es entonces existirán $y \neq y'$ tal que $xy = xy'$ y por lo tanto $x(y - y') = 0$, con lo cual hay divisores de cero, contrariamente a lo que establece el ser un dominio de integridad. Por otro lado, al ser $\mathcal{K}$ un cuerpo finito, el que f_x sea una inyección implica que es una biyección.

Existirá entonces, para cada x, un único elemento 1_x que cumple $f_x(1_x) = x$, y un único elemento x^{-1} que cumplirá $f_x(x^{-1}) = 1_x$. Sólo nos queda demostrar que todos los 1_x son iguales para mostrar que existe neutro y los inversos. Es decir, $1_x = 1_y$ para todo x, y. Para probar esto, consideremos que como f_x es una biyección, existe z tal que $xz = y$. Entonces, $(xz)1_x = (x1_x)z = xz$, de lo cual $1_x = 1_{xz} = 1_y$.

De modo que $\mathcal{K}[X]/(f)$ es un cuerpo de cardinalidad $|\mathcal{K}|^n$. Con esto podemos construír un cuerpo de cardinal potencia de primo, para toda potencia n y todo primo p. Tomamos el cuerpo $\mathcal{Z}_p$, tomamos un polinomio irreductible f de grado n, y el cuerpo que buscamos es $\mathcal{Z}_p[X]/(f)$. Para que esta prueba sea completa deberíamos mostrar que para todo cuerpo finito $\mathcal{K}$ y todo grado n existe un polinomio irreductible de grado n sobre $\mathcal{K}$. Esto no se probará.

Ejemplo: veamos un ejemplo de un cuerpo no primal. Tomaremos el cuerpo base $\mathcal{K} = F_5 \approx \mathcal{Z}_5$ y consideraremos la potencia 2. Para ello usaremos un polinomio irreductible (en $\mathcal{Z}_5$) de grado 2, a saber $f(x) = x^2 - 2$. El resultado será $F_5[X]/(f) \approx F_{25}$. Todos los elementos de este cuerpo son polinomios de grado 1 o menos, o sea son de la forma $a + bx$, con $a, b \in F_5$. Las operaciones se realizan primero operando los polinomios y luego tomando el resto de dividir por $f(x)$. Esto es

[3] Es decir que no se puede expresar como el producto de otros dos, ambos de grado menor que el de él.

[4] Es decir los polinomios módulo f: primero se realizan las operaciones como polinomios normales y luego se toma el resto de dividirlos por f.

equivalente a reemplazar x^2 por 2 donde aparezca[5]. Por ejemplo

$$(3+x)^2 \quad = \quad 9+6x+x^2 \quad = \quad 9+6x+2 \quad = \quad 11+6x \quad = \quad 1+x$$

(donde la última conversión corresponde a F_5 mismo). La inversión se realiza con el conocido truco

$$\frac{1}{1+x} \quad = \quad \frac{1-x}{(1+x)(1-x)} \quad = \quad \frac{1-x}{1-x^2} \quad = \quad \frac{1-x}{-1} \quad = \quad -1+x \quad = \quad 4+x\ .$$

En general, la inversión se puede realizar (aunque hay métodos más eficientes) con la regla $a^{-1} = a^{p^n-2}$, puesto que $a^{p^n-1} = 1$ según Fermat. Para ver esto es necesario extender la demostración del Pequeño Teorema de Fermat a grupos abelianos finitos $(G,\cdot)$, tales como $(F_{p^n} - \{0\},\cdot)$ en nuestro caso.

La demostración partía observando que, para todo $a \in G$, la función $f_a(x) = ax$ era una biyección en G (tal como lo hemos probado para ver que todo dominio de integridad es un cuerpo). De modo que

$$\prod_{x\in G} x \quad = \quad \prod_{x\in G} ax \quad = \quad a^{|G|}\prod_{x\in G} x$$

y dado que $\prod_{x\in G} x$ tiene inverso, se multiplica a ambos lados por ese inverso para obtener

$$1 = a^{|G|}$$

En nuestro caso, $|F_{p^n} - \{0\}| = p^n - 1$, de lo que se deduce la afirmación.

[5]En general, si $f(x) = \sum_{i=0}^{n} a_i x^i$, el módulo se obtiene reemplazando x^n por $-\sum_{i=0}^{n-1} a_n^{-1} a_i x^i$.