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

Cátedra No. 18 : 23 de Octubre

Transcriptor: Marcos Kiwi

1 Ejemplo de funciones de un sentido

Hemos dado definiciones formales de funciones de un sentido (fuertes y débiles), como también de colecciónes de funciones de un sentido (fuertes y débiles). Sin embargo, no hemos mostrado que estos tipos de funciones y colecciones de funciones existen. A continuación veremos que bajo ciertos supuestos, se puede garantizar dicha existencia. Probar la existencia incondicional de alguno de los tipos de funciones criptográficas que hemos estudiado es un problema que permanece abierto.

Por otro lado, sabemos que funciones fuertes de un sentido existen si y sólo si funciones débiles de un sentido existen. De aquí, que el siguiente resultado, de fácil demostración, implica que si alguna de las funciones o colección de funciones antes mencionada existen, entonces las otras también.

Teorema 1 *Existe una función de un sentido fuerte (respectivamente débil), si y sólo si, existe una colección de funciones de un sentido fuerte (respectivamente débil).*

Los siguientes supuestos nos permitirán garantizar la existencia de colecciónes de funciones de un sentido:

- **Supuesto fuerte acerca del logaritmo discreto:** Para todo polinomio q, cualquiera sea el adversario A, existe un entero no-negativo k_0, tal que si k es al menos k_0 se tiene que

$$\Pr\left[\, A(p,g,y) = x \text{ tal que } y \equiv g^x \pmod p, x \in \mathcal{Z}_{p-1} \,\right] \;\leq\; \frac{1}{q(n)}\,,$$

  donde la probabilidad es sobre los primos p tal que $|p| = k$,[1] los generadores g de $\mathcal{Z}_p^*$ y la fuente de aleatoreidad de A.

[1] En el resto de esta cátedra, si ϕ es una expresión denotaremos por $|\phi|$ la cantidad de bits necesarios para representar eficientemente ϕ, e.g. si n es un entero no-negativo $|n| = \lceil \log(n) \rceil$.

- **Supuesto débil acerca del logaritmo discreto:** Existe un polinomio q tal que cualquiera sea el adversario A, existe un entero no-negativo k_0, tal que si k es al menos k_0 se tiene que

$$\Pr\left[\, A(p,g,y) = x \text{ tal que } y \equiv g^x \pmod{p}, x \in \mathcal{Z}_{p-1} \,\right] \;\leq\; 1 - \frac{1}{q(k)}\,,$$

  donde la probabilidad es sobre los primos p tal que $|p| = k$, los generadores g de $\mathcal{Z}_p^*$ y la fuente de aleatoreidad de A.

La demostración de que los supuestos anteriores implican la existencia de colecciones de funciones de un sentido se basa en los siguientes resultados, que además son de interés por si mismos.

Lema 1 *Si p es un primo, entonces g es un generador de $\mathcal{Z}_p^*$, si y sólo si, cualquiera sea q primo tal que $q|(p-1)$ se tiene que $g^{p-1/q} \not\equiv 1 \pmod{p}$.*

Dem: Supongamos que g es generador de $\mathcal{Z}_p^*$. Claramente si $q|(p-1)$, entonces $g^{(p-1)/q} \equiv 1 \pmod{p}$ contradice el hecho que g tiene orden $(p-1)$, luego se debe tener que $g^{(p-1)/q} \not\equiv 1 \pmod{p}$ cualquiera sea el divisor q de $(p-1)$.

Por otro lado, supongamos que $g^{(p-1)/q} \not\equiv 1 \pmod{p}$ cualquiera sea q primo tal que $q|(p-1)$. Si g no fuese generador de $\mathcal{Z}_p^*$ entonces se tendría que el subgrupo cíclico de $\mathcal{Z}_p^*$ generado por g tiene un orden $k < p-1$ tal que $k|(p-1)$ (por el Teorema de Lagrange). Sea q el menor primo que divide a $s = \frac{p-1}{k}$, notar que dicho primo existe pues $s > 1$. Sigue que $g^{(p-1)/q} \equiv (g^k)^{s/q} \equiv 1 \pmod{p}$, lo que constituye una contradicción. □

Lema 2 *Existe un algoritmo del tipo Las Vegas que dado p primo y la factorización de $p-1$ encuentra un generador de $\mathcal{Z}_p^*$.*

Dem: Sea p primo, y supongamos conocidos los q_i primos y e_i enteros tales que $p - 1 = \prod_{i=1}^{k} q_i^{e_i}$. Recordemos que $\mathcal{Z}_p^*$ posee $\varphi(p-1)$ generadores distintos. Luego, del Lema 1 el algoritmo descrito a continuación tiene una probabilidad igual a $\varphi(p-1)/(p-1)$ de encontrar un generador de $\mathcal{Z}_p^*$.

1. Elegir $g \in \mathcal{Z}_p^*$ al azar.
2. Si para todo $i \in \{1, \ldots, k\}$, $g^{(p-1)/q_i} \not\equiv 1 \pmod{p}$,
   entonces

   g es un generador de $\mathcal{Z}_p^*$

   en caso contrario

   parar (fracaso).

Iterando el algoritmo anterior se obtiene el resultado deseado después de observar que $\varphi(m)$ es al menos igual al número de primos menores que m, que conjuntamente con el Teorema de los Números Primos implica que $\varphi(p-1) = \Omega(p/\log(p-1))$,[2] es decir $\varphi(p-1)/(p-1) = \Omega(1/\log(p-1))$. □

Teorema 2 *Bajo el supuesto fuerte (respectivamente débil) acerca del logaritmo discreto existe una colección de funciones de un sentido fuerte (respectivamente débil).*

Dem: Sea el conjunto de índices $I = \{(p,g) \,|\, p \text{ primo }, g \text{ generador de } \mathcal{Z}_p^*\}$, y el conjunto de funciones $EXP = \{EXP_{(p,g)}\colon \mathcal{Z}_{p-1} \to \mathcal{Z}_p^* \,|\, (p,g) \in I, EXP_{(p,g)}(x) = g^x \bmod p\}$. Veamos que EXP es una colección de funciones de un sentido fuerte.

1. Sea S_1 la máquina de Turing probabilista que en la entrada 1^k elije un primo p y un generador g de $\mathcal{Z}_p^*$ tal que $|(p,g)| = k$. (La máquina S_1 existe pues mediante un algoritmo del tipo Las Vegas conocido[3] se puede encontrar un primo p de un tamaño dado junto con la factorización de $p-1$, y por el Lema 2 también sabemos existe un algoritmo del tipo Las Vegas que dado p primo y la factorización de $p-1$ encuentra un generador de $\mathcal{Z}_p^*$.)
2. Sea S_2 la máquina probabilista que en la entrada (p,g) elije al azar (uniformemente) un elemento de $\mathcal{Z}_{p-1}$.

[2] Más aun, se sabe que $\varphi(m) > m/(6 \log\log m)$ (J. Rosser y L. Schoenfeld, *Approximate Formulas for Some Functions of Prime Numbers*, Illinois Journal of Mathematics, Volume 6, 1962, páginas 64–94).

[3] (E. Bach, *How to Generate Factored Random Numbers*, SIAM Journal co Computing, Volume 17, 1988, páginas 179–193).

3. Sea A' la máquina de Turing polinomial determinista que en la entrada (p,g) y $x \in \mathcal{Z}_{p-1}$ calcula mediante el método de cuadrados iterados $EXP_{(p,g)}(x) = g^x \bmod p$.

Claramente, bajo el supuesto fuerte acerca del logaritmo discreto se tiene que para todo polinomio q, cualquiera sea el adversario A, existe un entero no-negativo k_0, tal que si k es al menos k_0 se tiene que

$$\Pr\Big[\, A((p,g), EXP_{(p,g)}(x)) = x \,\Big] \;\leq\; \frac{1}{q(k)}\,,$$

donde la probabilidad es sobre los $(p,g) \in I$ elegidos por S_1 en la entrada 1^k, los $x \in \mathcal{Z}_{p-1}$ elegidos por S_2 en la entrada (p,g), y la fuente de aleatoreidad de A. $\square$

2 Colección de funciones de un sentido de puerta secreta

Para construir un criptosistema de clave pública no sólo se requiere contar con una función de un sentido. No queremos que la función de encripción sea de un sentido para el legítimo destinatario de los mensajes encriptados. Es necesario que el legítimo destinatario de los mensajes encriptados pueda decriptar con la ayuda de cierta información secreta que sólo él posee, i.e. con la ayuda de una puerta secreta. Informalmente decimos que una función es de un sentido de puerta secreta si es de un sentido, pero es fácil de invertir si se posee cierta información adicional.

A continuación formalmente definimos lo que es una familia de funciones de un sentido de puerta secreta.

Definición 1 *Sea I un conjunto de índices. Para todo $i \in I$ sean D_i y R_i conjuntos finitos. Una colección de funciones de un sentido fuerte (respectivamente débil) de puerta secreta es un conjunto*

$$F \;=\; \{f_i\colon\, D_i \to R_i \,|\, i \in I\}\,,$$

tal que

1. *Existe un polinomio p y una máquina de Turing probabilista M_1 que en la entrada 1^k encuentra una tupla (i, t_i) donde $|i| = k$, $|t_i| \leq p(k)$. La información t_i se denomina puerta secreta.*

2. *Existe una máquina de Turing probabilista M_2 que en la entrada $i \in I$ encuentra $x \in D_i$.*

3. *Existe una máquina de Turing probabilista M tal que para todo $i \in I$, $x \in D_i$, $M(i,x) = f_i(x)$.*

4. **Caso fuerte:** *para todo adversario A, para todo polinomio q, existe un entero no-negativo k_0 tal que para todo $k > k_0$*

$$\Pr\left[A(i, f_i(x)) \in f_i^{-1}(f_i(x)) \right] \;\leq\; \frac{1}{q(k)},$$

donde la probabilidad se toma sobre todos los i elegidos por M_1 sobre la entrada 1^k, los x elegidos por M_2 sobre la entrada i y la fuente de aleatoreidad de A.

   Caso débil: *existe un polinomio q, tal que para cualquier adversario A, existe un entero no-negativo k_0 tal que para todo $k > k_0$*

$$\Pr\left[A(i, f_i(x)) \in f_i^{-1}(f_i(x)) \right] \;\leq\; 1 - \frac{1}{q(k)},$$

donde la probabilidad se toma sobre todos los i elegidos por M_1 sobre la entrada 1^k, los x elegidos por M_2 sobre la entrada i y la fuente de aleatoreidad de A.

5. *Existe una máquina de Turing probabilista M' tal que para todo $i \in I$, $x \in D_i$, $M'(i, t_i, f_i(x)) = x$, i.e. f_i es fácil de invertir cuando t_i es conocido.*

Al igual que en la sección anterior veremos que bajo ciertos supuestos podemos exhibir ejemplos de colecciones de funciones de un sentido de puerta secreta. Primero enunciemos cuales son estos supuestos.

- **Supuesto fuerte acerca de RSA:** Sea $H_k = \{n = pq \,|\, p, q \text{ primos}, |p| \approx |q|\}$. Para todo polinomio q, cualquiera sea el adversario A, existe un entero no-negativo k_0, tal que si k es al menos k_0 se tiene que

$$\Pr\left[A(n, e, RSA_{n,e}(x)) = x \right] \;\leq\; \frac{1}{q(k)},$$

  donde la probabilidad es sobre los $n \in H_k$, los $e \in \mathcal{Z}^*_{\varphi(n)}$, los $x \in \mathcal{Z}_n$ y la fuente de aleatoreidad de A

- **Supuesto débil acerca de RSA:** Sea $H_k = \{n = pq \,|\, p, q \text{ primos}, |p| \approx |q|\}$. Existe un polinomio q tal que cualquiera sea el adversario A, existe un entero no-negativo k_0, tal que si k es al menos k_0 se tiene que

$$\Pr\left[A(n, e, RSA_{n,e}(x)) = x \right] \;\leq\; 1 - \frac{1}{q(k)},$$

donde la probabilidad es sobre los $n \in H_k$, los $e \in \mathcal{Z}^*_{\varphi(n)}$, los $x \in \mathcal{Z}_n$ y la fuente de aleatoreidad de A.

Definamos entonces el conjunto de índices

$$I \;=\; \{(n,e) \mid n = pq, p \text{ y } q \text{ primos tales que } |p| \approx |q|, e \in \mathcal{Z}^*_{\varphi(n)}\},$$

y el conjunto de funciones

$$RSA \;=\; \{RSA_{n,e}\colon\ \mathcal{Z}_n \to \mathcal{Z}_n \mid (n,e) \in I, RSA_{n,e}(x) = x^e \bmod n\}.$$

Del estudio que ya hemos realizado acerca del criptosistema de RSA es fácil ver que se tiene el siguiente resultado.

Teorema 3 *Bajo el supuesto fuerte (respectivamente débil) acerca de* RSA*, RSA es una colección de funciones de un sentido fuerte (respectivamente débil) de puerta secreta.*