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

Cátedra No. 8 : 28 de Agosto

Transcriptor: Jens Hardings

1 Criptografía Moderna o de Clave Pública

En los criptosistemas vistos hasta ahora, Alicia y Roberto eligen la clave K en secreto, comunicándola a través de un canal seguro. Esta clave permite generar una regla de encripción e_K y una regla de decripción d_K. En los criptosistemas que hemos estudiado, d_K es fácilmente derivable al conocer e_K. Los criptosistemas de este tipo se conocen con el nombre de criptosistemas de clave privada.

Evidentemente, al usar este tipo de sistemas se depende de la existencia previa (aunque sea temporal) de un canal seguro, en el cual Alicia y Roberto se comunican la clave, para luego poder mandar información a través de otro canal inseguro.

En cambio, la criptografía de clave pública se basa en la idea que quizás es posible encontrar un criptosistema en que es computacionalmente infactible determinar d_K dado e_K. En ese caso, e_K puede ser publicada por Roberto, y Alicia o cualquier otro individuo puede enviar mensajes encriptados a Roberto usando e_K y este último será la única persona capaz de decriptar el texto cifrado usando su regla de decripción secreta d_K.

La idea de la criptografía pública se debe a Diffie y Hellman [1976], los cuales no dieron un ejemplo de criptosistema de este tipo. Ellos propusieron que podía construirse un criptosistema de este tipo si era posible encontrar una función "fácil" de calcular, pero "difícil" de invertir. La primera realización de criptosistema público se debe a Rivest, Shamir y Adleman [1977].

Es importante notar que un criptosistema de clave pública no podrá jamás ser un criptosistema perfectamente secreto. En efecto, conocido el texto cifrado, un adversario puede encriptar todos los textos planos y determinar cual es el único tal que $y = e_K(x)$, dado que el adversario conoce e_K. Luego, el texto cifrado enviado permite identificar completamente el texto plano. Por lo tanto, la discusión de la seguridad de los criptosistemas de clave pública necesariamente debe hacerse en el ámbito de la seguridad computacional, i.e. la dificultad computacional de calcular d_K conociendo e_K.

2 Funciones de sentido único y de puerta secreta

La noción detrás de las funciones de sentido único es que se tiene una función $f : \mathcal{P} \longrightarrow \mathcal{C}$ tal que

- f es fácil de calcular
- f^{-1} no es tan fácil de calcular

Esta abstracción es útil al hablar de criptosistemas de clave pública. Más adelante formalizamos la noción de funciones de un sólo sentido.

No se conoce la existencia de estas funciones, sin embargo existen conjeturas acerca de posibles candidatos:

- Factorización

  $f : N \times N \rightarrow N$

  $(m, n) \mapsto m \cdot n$

  Si el dominio de esta función se restringe a los pares (m, n) tales que m y n son primos, f tiene inversa y se supone que es difícil de calcular. La razón por la cual se considera "difícil" de invertir esta función es que, después de mucho tiempo de investigación, el algoritmo conocido más eficiente para factorizar (y por ende invertir f) se demora $e^{(1{,}92+o(1))(lg(n))^{\frac{1}{3}}(lg(lg(n)))^{\frac{2}{3}}}$

- Logaritmo Discreto

  Sea p un primo, $\mathcal{Z}_p^* = \mathcal{Z}_p \setminus \{0\}$ es un grupo multiplicativo y es cíclico, i.e. existe g en $\mathcal{Z}_p^*$ tal que $\mathcal{Z}_p^* = \{g^i \,|\, i \in \{1, 2, \cdots, p-1\}\}$. Sea $f(p, g, i) = (g^i \bmod p, q, g)$, donde p es primo, i es un entero no negativo y g es generador de $\mathcal{Z}_p^*$.

  Se presume que $f(\cdot, \cdot, \cdot)$ es de sentido único, ya que el mejor algoritmo conocido para calcular la inversa (el *logaritmo discreto*) toma $O(e^{(lg(p) \cdot lg(lg(p)))^{\frac{1}{2}}})$

  Observación: $f(\cdot, \cdot, \cdot)$ se puede calcular eficientemente por el método de los cuadrados iterados que veremos más adelante.

Pero la criptografía de clave pública requiere más que una función de un sentido. La regla de encripción e_K debe ser fácil de invertir para quien la publica.

Se requieren funciones de un sentido con puerta secreta, i.e. tales que cierta información (que no se publica) las hagan fáciles de invertir.

3 RSA

RSA es el criptosistema de clave pública ideado por Rivest, Shamir y Adleman. En este sistema, $\mathcal{P} = \mathcal{C} = \mathcal{Z}_n$, $n = p \cdot q$ donde p y q son primos impares. Además $\mathcal{K} = \{(p, q, a, b) \,|\, n = p \cdot q \text{ y } ab \equiv 1(\mathrm{mod}\varphi(n))\}$, donde $\varphi(n)$ es la función phi de Euler, y

$$\begin{aligned} e_K &= x^a \bmod n \\ d_K &= y^b \bmod n. \end{aligned}$$

La clave pública es (n, a).

El sistema se basa en la suposición que $f(n, a, x) = (x^a \bmod n, n, a)$ es una función de sentido único.

Además, la puerta secreta que permite decriptar de manera "fácil" es el conocimiento de p y q, y luego de $\varphi(n) = (p-1)(q-1)$. Por lo tanto, si a es primo relativo a $\varphi(n)$, podemos calcular el exponente de decripción b por el algoritmo de Euclides. Observar que para que $d_K(e_K(x)) = x$, se debe tener que $x = x^{ab} \bmod n, \forall x \in \mathcal{Z}_n$ si $ab \equiv 1(\mathrm{mod}\varphi(n))$. No estamos en condiciones de probar esto último. Para ello requerimos ahondar en teoría de números.

4 Más de teoría de números

Teorema 1 *El pequeño teorema de Fermat*

Sea p un primo. Entonces, para todo entero a, $a^p \equiv a(\mathrm{mod}p)$ y si a no es divisible por p, entonces $a^{p-1} \equiv 1(\mathrm{mod}p)$.

Dem: Sea a divisible por p. Entonces $a \equiv 0(\mathrm{mod}p)$ y $a^p \equiv 0(\mathrm{mod}p)$ por lo que $a^p \equiv a(\mathrm{mod}p)$.

Si p no divide a a tenemos que $|\{ia \bmod p \,|\, i \in \{1, ..., p-1\}\}| = p - 1$. En efecto, si i es distinto de j y $ia \equiv ja(\mathrm{mod}p)$, entonces p divide a $a(i-j)$. Como p es primo, p no divide a a, y p es primo relativo con a, tenemos que $p \mid (i-j)$, lo cual contradice el supuesto anterior.

Luego, el conjunto $\{ia \bmod p \,|\, i \in \{1, ..., p-1\}\} = \mathcal{Z}_p^*$

$$\prod_{i=1}^{p-1} i \equiv \prod_{i=1}^{p-1} (ia)(\mathrm{mod}p)$$

$$a^{p-1}\prod_{i=1}^{p-1} i \equiv \prod_{i=1}^{p-1} i$$

Como $\prod_{i=1}^{p-1} i$ es primo relativo con p, se puede cancelar en ambos lados y obtenemos $a^{p-1} \equiv 1(\mathrm{mod} p)$

Inmediatamente se ve que $a^p \equiv a(\mathrm{mod} p)$ □

Corolario 1 *Si a no es divisible por p y $n \equiv m(\mathrm{mod}(p-1))$, entonces $a^n \equiv a^m(\mathrm{mod} p)$.*

Dem: Si $n \equiv m(\mathrm{mod} p-1)$, entonces se cumple que existe un entero b tal que $n = m + b(p-1)$. Por lo tanto, $a^n = a^{m+b(p-1)} = a^m \cdot a^{b(p-1)}$ y del teorema anterior se tiene que $a^{b(p-1)} \equiv (a^{p-1})^b \equiv 1(\mathrm{mod} p)$, y entonces $a^n \equiv a^m(\mathrm{mod} p)$. □

Teorema 2 *Euler*

Si a es primo relativo con n, entonces $a^{\varphi(n)} \equiv 1(\mathrm{mod} n)$.

Dem: Primero se demostrará el teorema en el caso de que n es una potencia de un primo p, o sea que $n = p^\alpha$. Para ello usaremos inducción sobre α. El caso $\alpha = 1$ ya se demostró anteriormente (pequeño Teorema de Fermat). Suponiendo que $\alpha \geq 2$, y que se cumple el teorema para $n = p^{\alpha-1}$, entonces $a^{p^{\alpha-1}-p^{\alpha-2}} = 1 + p^{\alpha-1}b$ para algún entero b. Usando el hecho de que los coeficientes binomiales de $(1+x)^p$ son divisibles por p, exceptuando 1 y x en los extremos[1], se puede elevar a p a ambos lados y se llega a $a^{p^\alpha-p^{\alpha-1}} = 1 + S$, donde S es una suma de términos todos divisibles por p. Entonces se tiene que $a^{\varphi(p^\alpha)} - 1$ es divisible por p, dado que como hemos visto anterioemante, $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$.

Finalmente, como φ es multiplicativa, es claro que $a^{\varphi(n)} \equiv 1(\mathrm{mod} p^\alpha)$.

En el caso general, existen m distintos p_i (todos primos) y e_i, m un natural, tales que

$$\begin{aligned} n &= \prod_{i=1}^{m} p_i^{e_i} \\ \varphi(n) &= \prod_{i=1}^{m} \varphi(p_i^{e_i}) \end{aligned}$$

[1]Al expandir, se ve que los términos son de la forma $\binom{p}{i}x^i$, con $1 < i < p$, los cuales son claramente divisibles por p.

Definamos
$$b_j = \prod_{i=1}^{j} p_i^{e_i} \ , con\ j = 1, ..., m.$$
Como b_{j-1} es primo relativo con $p_j^{e_j}$, se puede ocupar la parte anterior de la demostración para cada b_j, entonces:
$$\begin{array}{rcl} a^{\varphi(b_1)} = & a^{\varphi(p_1^{e_1})} & \equiv 1(\mathrm{mod} p_1^{e_1}) \\ & \vdots & \\ a^{\varphi(b_j)} = & (a^{\varphi(b_{j-1})})^{\varphi(p_j^{e_j})} & \equiv 1(\mathrm{mod} p_j^{e_j}), \end{array}$$
o sea que $a^{\varphi(n)} \equiv 1(\mathrm{mod} p_j^{e_j})$ para $j = 1, ..., m$. Entonces, podemos afirmar que
$$a^{\varphi(n)} \equiv 1(\mathrm{mod} \prod_{i=1}^{n} p_i^{e_i})$$
y se concluye que $a^{\varphi(n)} \equiv 1(\mathrm{mod} n)$. □

Corolario 2 *Si a es primo relativo con n, y $m \equiv m'(\mathrm{mod} \varphi(n))$, entonces $a^m \equiv a^n(\mathrm{mod} n)$.*

Dem: Del teorema anterior tenemos que $a^{\varphi(n)} \equiv 1(\mathrm{mod} n)$. Además, $m \equiv n(\mathrm{mod}\ \varphi(n))$, o sea que $m = t\varphi(n) + n$, para algún entero t. Entonces, $a^m \equiv a^{t\varphi(n)+n} \equiv (a^{\varphi(n)})^t \cdot a^n \equiv a^n(\mathrm{mod} n)$. □

Teorema 3 *Teorema chino del resto*

Supongamos que queremos resolver
$$\begin{array}{rcl} x & \equiv & a_1(\mathrm{mod} m_1) \\ x & \equiv & a_2(\mathrm{mod} m_2) \\ x & \equiv & a_3(\mathrm{mod} m_3) \\ & \vdots & \\ x & \equiv & a_r(\mathrm{mod} m_r) \end{array}$$
donde m_i y m_j son primos relativos si $i \neq j$.

Entonces, existe una solución x que satisface todas las ecuaciones anteriores y cualquiera dos soluciones del sistema anterior son congruentes módulo $M \equiv m_1 \cdot m_2 \cdot \ldots \cdot m_r$

Dem: Unicidad: Sean x y x' dos soluciones, luego

$$\begin{aligned} x &\equiv a_i (\mathrm{mod} m_i) \\ x' &\equiv a_i (\mathrm{mod} m_i) \end{aligned}$$

donde $i = 1 \ldots r$. Luego $(x - x') \equiv 0(\bmod m_i)$, donde $i = 1 \ldots r$. Y como m_i es primo relativo con m_j si $i \neq j$, sigue que $x \equiv x' (\mathrm{mod} M)$

Existencia: Sea $N_i = \frac{M}{m_i}$, luego N_i y m_i son primos relativos.

Por lo tanto existe un M_i tal que $N_i M_i \equiv 1 (\mathrm{mod} m_i)$. Luego

$$x = \sum_{i=1}^{r} a_i N_i M_i \bmod M.$$

Se tiene que x es solución del sistema de congruencias, puesto que

$$\begin{aligned} x &\equiv \sum_{j=1}^{r} a_j N_j M_j (\mathrm{mod} m_i) \\ &\equiv a_i N_i M_i (\mathrm{mod} m_i) \\ &\equiv a_i (\mathrm{mod} m_i) \end{aligned}$$

□

Obs: Además de verificar el teorema, la demostración recién vista da un algoritmo eficiente para encontrar las soluciones del sistema de congruencias presentado.

Con esto ya tenemos los elementos necesarios para probar que $d_K(e_K(x)) = xi$ para cualquier $x \in \mathcal{P}$ en RSA.