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

Cátedra No. 10 : 14 de Abril

Transcriptor: Miguel Barrera M.[1]

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 un criptosistema público se debe a Rivest, Shamir y Adleman [1977].

El hecho de que no se requiera un canal seguro para la comunicación de una clave secreta supone una ventaja con respecto a la criptografía de clave privada, y esta razón ha facilitado la propagación de la Criptografía de clave pública en medios masivos, como por ejemplo Internet o los mismos teléfonos portátiles.

Sin embargo 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.

[1] Basada en una transcripción anterior de Jens Hardings

2 Definición de criptosistema de clave pública

El escenario que consideraremos es uno en que hay $(U_1...U_n)$ usuarios con pares de claves $< P_n, S_n >$ donde P_n es público (conocido por los U_n usuarios) y S_n es secreto.

Definición 1 *un criptosistema de clave pública es un tripleta (G, E, D) de algoritmos probabilistas a tiempo polinomial esperado tal que.*

- *G es el algoritmo generador de claves:*

  Toma desde la entrada 1^k y produce un par (e, d) donde e es denominada clave publica y d es denominada clave secreta (notación $(e, d) \varepsilon G(1^k)$).

  También nos referiremos a (e, d) como par de claves de encripción/decripción.

- *E es el algoritmo de encripción:*

  Este algoritmo toma como entrada 1^k, una clave pública e, un mensaje $m \varepsilon \{0, 1\}^k$ y produce como salida $c \varepsilon \{0, 1\}^*$ llamado texto cifrado.

  Notación:

  $c \varepsilon E(1^k, e, m)$ *o* $c \varepsilon E(e, m)$ *o* $c \varepsilon E(m)$

  nota: se usaran estas dos últimas, cuando sea claro por contexto.

- *D Algoritmo de decripción :*

  El algoritmo toma 1^k una clave publica e , una clave privada d y $c \varepsilon E(1^k, e, m)$ y produce como salida $m \varepsilon \{0, 1\}^*$ tal que $\forall (e, d) \varepsilon G(1^k)$, $\forall c \varepsilon E(1^k, e, m)$ $Pr[D(1^k, e, d, c) \neq m]$ es despreciable.

  Es decir, se acepta que la decripción no sea única.

Convención

Extendemos la notación de forma que $E(\alpha_1...\alpha_{l+1})$=$E(\alpha_1)...E(\alpha_l)E(\alpha_{l+1}\ P)$.

Donde P hace padding para completar el bloque y donde $\alpha_1...\alpha_l, \alpha_{l+1}P \varepsilon \{0, 1\}^k$

3 RSA

RSA es el criptosistema de clave pública ideado por Rivest, Shamir y Adleman. En este sistema, el conjunto de claves

$\mathcal{K} = \{(n, e, d) \,|\, n = p \cdot q$ $(p, q$ primos$)$ y $e, d \varepsilon \mathcal{Z}_{\varphi(n)}$ son tales que $e \cdot d \equiv 1(\mathrm{mod}\varphi(n))\}$,

donde $\varphi(n)$ es la función phi de Euler, y si K $= (n, e, d) \varepsilon \mathcal{K}$

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

La clave pública es (n, e) y la clave privada es d.

Observar que para que $d_K(e_K(x)) = x$, se debe tener que $x = x^{e \cdot d} \bmod n, \forall x \in \mathcal{Z}_n$ si $e \cdot d \equiv 1 (\mathrm{mod} \varphi(n))$. No estamos en condiciones de probar esto último. Para ello requerimos ahondar en teoría de números (ver la sección 4).

Ejemplo 1

Ahora vamos a dar un ejemplo de uso de un criptosistema RSA:

Supongamos que Roberto elige $p = 101$ y $q = 113$. Entonces $n = 11413$ y
$\varphi(n) = 100 \cdot 112 = 11200$.

Como $11200 = 2^6 5^2 7$ cualquier entero e puede ser usado como un exponente de encripción, si y solo si e no fuera divisible por 2, 5 o 7. (No se debe factorizar $\varphi(n)$, solo hay que verificar que $\mathrm{mcd}(\varphi(n), e)$=1 usando el algoritmo del Euclides).

Supongamos que roberto elige e=3533. Entonces del algoritmo de Euclides resulta:

$$e^{-1} = 6597 \bmod 11200$$

Luego, la clave secreta de roberto es d=6597

Roberto publica n= 11413 y e=3533. Ahora supongamos que Alicia quiere enviar a Roberto el texto 9726. Ella calculará:

$$9726^{3533} \bmod 11413 = 5761$$

y enviará el texto cifrado 5761 por cualquier canal hasta Roberto. Cuando Roberto reciba el mensaje, el usará su clave secreta y calculará:

$$5761^{6597} \bmod 11413 = 9726$$

Esta instancia de RSA es fácil de atacar porque p y q son números pequeños, entonces la factorizacion de $\varphi(n)$ es posible.

Hay algoritmos computacionales que factorizan hasta un número de 130 cifras en un tiempo corto (horas en máquinas modernas), por lo cual se recomienda que la elección de los p y q, tenga cada uno 100 cifras, con lo que n tendría unas 200 cifras, número cuya factorización no es computacionalmente factible (en el sentido del tiempo empleado, en estos algoritmos el tiempo de espera crece muy rápido).

4 Más de teoría de números

Congruencias

En esta sección repasaremos algunos resultados básicos que conciernen a las congruencias.

Dados tres enteros a, b, m decimos que *a es congruente a b módulo m* si $m|(a-b)$ y lo denotamos $a \equiv b \pmod m$ o $a \equiv_m b$

Sea $\mathcal{Z}_m$ el conjunto $\{0, \ldots, m-1\}$ dotado de dos leyes de composición interna: suma $(+)$ y multiplicación $(\cdot)$, donde la suma y multiplicación son exactamente iguales a la suma y multiplicación de enteros pero donde los resultados son reducidos módulo m. Se verifica que $\mathcal{Z}_m$ así definido forma un anillo conmutativo con unidad.[2]

A continuación enumeramos algunas propiedades de las congruencias.

- Si $a \equiv_m b$ y $c \equiv_m d \Rightarrow a \pm c \equiv_m b \pm d$ y $a \cdot c \equiv_m b \cdot d$
- Si $a \equiv_m b$ y $d|m \Rightarrow a \equiv_d b$
- Si $a \equiv_m b$ y $a \equiv_n b$ y $mcd(n, m) = 1 \Rightarrow a \equiv_{n \cdot m} b$

Proposición 1 *Los elementos de $\mathcal{Z}_m$ que tienen inversos multiplicativos son aquellos que son relativamente primos a m. De hecho, de existir el inverso de $a \in \mathcal{Z}_m$ este se puede calcular en el tiempo que toma el algoritmo de Euclides en determinar* $\mathrm{mcd}(a, m)$.

Dem: Si $a \in \mathcal{Z}_m$ no es relativamente primo a m entonces $d = \mathrm{mcd}(a, m) > 1$. Supongamos que existe un $b \in \mathcal{Z}_m$ tal que $ab \equiv 1 \pmod m$. Luego $ab - 1$ es divisible por d, pero $d|a$, por lo tanto concluimos que 1 es divisible por d, contradicción.

Si $a \in \mathcal{Z}_m$ es relativamente primo a m entonces por un corolario anterior que decía que si a y m eran primos relativos, entonces existen enteros u y v tales que $1 = au + mv$. Eligiendo $b = u$, sigue que $m|(1 - ab)$, i.e. $ab \equiv 1 \pmod m$. Luego, $b \bmod m \in \mathcal{Z}_m$ es inverso multiplicativo de a. $\square$

Corolario 1 *La ecuación $ax \equiv b \pmod m$ en la indeterminada x tiene solución en $\mathcal{Z}_m$ si a y m son primos relativos y el tiempo que toma calcular sus soluciones esta dominado por el tiempo que toma encontrar inversos en $\mathcal{Z}_m$. Si $d = \mathrm{mcd}(a, m) > 1$ entonces $ax \equiv b \pmod m$ tiene solución en $\mathcal{Z}_m$ ssi $d|b$ y sus soluciones son las mismas que las de la ecuación $a'x \equiv b' \pmod{m'}$ donde $a' = a/d$, $b' = b/d$ y $m' = m/d$.*

[2] Recordemos que una estructura $(A, +, *)$ es una estructura de anillo conmutativo con unidad, si se cumplen las propiedades siguientes:
$(A, +)$ es una estructura de grupo abeliano
$(x \cdot y) \cdot z = x \cdot (y \cdot z)$, $\forall\, x, y, z \in A$ (Asociativa).
$x \cdot (y + z) = x \cdot y + x \cdot z$; $(x + y) \cdot z = x \cdot z + y \cdot z$ $\forall x, y, z \in A$ (Distributiva).
$\exists\, 1 \in A|\ x \cdot 1 = 1 \cdot x = x$, $x \in A$ (Existencia de elemento unidad)
$x \cdot y = y \cdot x$, $\forall\, x, y \in A$ (Conmutativa)

Dem: Claramente la solución en $\mathcal{Z}_m$ de la ecuación $ax \equiv$ b (mod m) es $x = a^{-1}b \bmod m$ donde a es el inverso multiplicativo de $a \in \mathcal{Z}_m$ que existe puesto que a y m son primos relativos y por la Proposición 1.

Si x es solución de $ax \equiv$ b (mod m) y $d = \text{mcd}(a, b)$ entonces $ax \equiv$ b (mod d). Luego $d|(ax - b)$. Pero como además $d|a$ se concluye que $d|b$. Por otro lado, $ax \equiv$ b (mod m) implica que $ax = b + km$ para algń entero k. Luego, $a'x = b' - km'$, i.e.

$a'x \equiv b'$ (mod m'). En el sentido inverso, tenemos que si $d|b$ entonces b' es un entero y como a' y m' son primos relativos existe un x solución de $a'x \equiv b'$ (mod m'). Luego, $a'x = b' - km'$ para algún entero k. Sigue que $ax = b - km$, i.e. $ax \equiv$ b (mod m). $\square$

Definición 2 *Dado G grupo, llamamos orden de G a la cantidad de elementos en G y se denota $|G|$.*

Definición 3 *Se define $\mathcal{Z}_n^*$ como el conjunto de números que pertencen a $\mathcal{Z}_n$ y que son primos relativos con n, por lo tanto*

$$\mathcal{Z}_n^* = \{m\varepsilon\{1, ..., n-1\}/mcd(n, m) = 1\}$$

Proposición 2 *$\mathcal{Z}_n^*$ es un grupo abeliano.*

Dem:

Cerradura: Es fácil ver que xy es primo relativo con n siempre que x e y sean primos relativos con n (no comparten factores y al multiplicarlos tampoco).

Asociatividad: Se hereda de la asociatividad en $\mathcal{Z}_n$.

Conmutatividad: Se hereda de la conmutatividad en $\mathcal{Z}_n$.

Elemento neutro: El 1, heredado también del neutro multiplicativo en $\mathcal{Z}_n$.

Elemento inverso: Por demostrar que $a \; \varepsilon \; \mathcal{Z}_n^* \Rightarrow a^{-1} \; \varepsilon \; \mathcal{Z}_n^*$.

Podemos observar que si $a \; \varepsilon \; \mathcal{Z}_n^*$ entonces es invertible en $\mathcal{Z}_n$, luego $\exists \; a^{-1} \; \varepsilon \; \mathcal{Z}_n$.

Debemos probar que $a^{-1} \; \varepsilon \; \mathcal{Z}_n^*$, i.e. mcd($a^{-1}$,$n$)=1

En efecto, si $a \cdot a^{-1} \equiv 1(\text{mod } n)$ entonces $n|(aa^{-1} - 1)$

Supongamos ahora que $\exists \; d \mid 1 < d < n$ y que $d|a^{-1}$ y $d|n$

pero $aa^{-1} - 1 = kn \Rightarrow aa^{-1} - kn = 1$ como $d|(aa^{-1} - kn) \Rightarrow d|1 \Rightarrow d = 1$

esto último está en contradicción con el hecho de que d >1

entonces tenemos que mcd(a^{-1},n)=1

y por lo tanto $a^{-1} \; \varepsilon \; \mathcal{Z}_n^*$.

$\square$

Teorema 1 *El pequeño teorema de Fermat*

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

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

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 $ia \equiv ja(\text{mod}p)$, 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 $\{ia \bmod p \,|\, i \in \{1, ..., p-1\}\} = \mathcal{Z}_p^*$

$$\begin{aligned} \prod_{i=1}^{p-1} i &\equiv \prod_{i=1}^{p-1} (ia)(\text{mod}p) \\ a^{p-1} \prod_{i=1}^{p-1} i &\equiv \prod_{i=1}^{p-1} i \end{aligned}$$

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 2 *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:

si mcd(a, n)=1, entonces la función definida desde $\mathcal{Z}_m^*$ a $\mathcal{Z}_m^*$ tal que a i le asigna la imagen $i \cdot a$ es invertible, en particular es biyectiva.

Debido a esto podemos establecer las siguientes igualdades

$$\prod_{i \varepsilon \mathcal{Z}_m^*} i \equiv_m \prod_{i \varepsilon \mathcal{Z}_m^*} (i \cdot a) \equiv_m a^{\varphi(n)} \cdot \prod_{i \varepsilon \mathcal{Z}_m^*} i$$

Luego se pueden cancelar las pitatorias del primer y tercer término, debido a que estamos en un grupo abeliano.

De esto último resulta $a^{\varphi(n)} \equiv_m 1$

□

Dem. alternativa: 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[3], 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 anteriormente, $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$.

[3] 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.

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

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

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

Definamos

$$b_j = \prod_{i=1}^{j} p_i^{e_i} \text{ , } con\ j = 1, ..., m.$$

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:

$$\begin{aligned} a^{\varphi(b_1)} = &\quad a^{\varphi(p_1^{e_1})} &\equiv 1(\text{mod} p_1^{e_1}) \\ &\quad \vdots & \\ a^{\varphi(b_j)} = &\quad (a^{\varphi(b_{j-1})})^{\varphi(p_j^{e_j})} &\equiv 1(\text{mod} p_j^{e_j}), \end{aligned}$$

o sea que $a^{\varphi(n)} \equiv 1(\text{mod} p_j^{e_j})$ para $j = 1, ..., m$. Entonces, podemos afirmar que

$$a^{\varphi(n)} \equiv 1(\text{mod} \prod_{i=1}^{n} p_i^{e_i})$$

y se concluye que $a^{\varphi(n)} \equiv 1(\text{mod} n)$.

$\square$

Corolario 3 *Si a es primo relativo con n, y $m \equiv m'(\text{mod}\varphi(n))$, entonces* $a^m \equiv a^n(\text{mod} n)$.

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