Criptografía de clave pública

El logaritmo discreto
Intercambio de claves de Diffie-Hellman
Criptosistema El Gamal

eman ta zabal zazu
Universidad del País Vasco
Euskal Herriko Unibertsitatea

KISA

Logaritmo discreto

Definición

Dados enteros a, b, n, c, *con* $0 \leq c \leq n-1$, *se dice que* c *es* un logaritmo discreto de a en base b módulo n *si*

$$a \equiv b^c \mod n.$$

Se escribe

$$c = \log_b a \mod n.$$

Problemas:

- Cuándo existe $\log_b a \mod n$.
- Cómo calcularlo.

  No se conocen algoritmos eficientes para calcular en tiempo polinómico logaritmos discretos, de ahí que puedan ser utilizados para desarrollar criptografía de clave pública.

Sea p un número primo.
Sabemos que $(\mathbb{Z}_p^*, \cdot)$ es un grupo de $p-1$ elementos.

El número de elementos de un grupo es el *orden* del grupo $(\mathrm{ord}(\mathbb{Z}_p^*) = p-1)$.

Además:

- Es un *grupo cíclico:* Existe $g \in \mathbb{Z}_p^*$ tal que cualquier elemento del grupo es potencia de g, es decir,

  $$\forall w \in \mathbb{Z}_p^*, \quad w \equiv g^s \mod p \quad \text{para algún entero } s.$$

  Al elemento g se le llama *generador* de $\mathbb{Z}_p^*$.
- Hay $\phi(p-1)$ generadores de $\mathbb{Z}_p^*$.

Observación: Si g es un generador de $\mathbb{Z}_p^*$, entonces cualquier elemento de $\mathbb{Z}_p^*$ posee logaritmo discreto en base g módulo p:

$$w \equiv g^s \mod p \Leftrightarrow \log_g w = s \mod p.$$

Ejemplo

$\mathbb{Z}_7^* = \{1, 2, 3, 4, 5, 6\}$ tiene $\phi(6) = 2$ generadores: 5 y 3.

$$
\begin{array}{lll}
5^0 \equiv 1 \mod 7, & 5^1 \equiv 5 \mod 7, & 5^2 \equiv 4 \mod 7, \\
5^3 \equiv 6 \mod 7, & 5^4 \equiv 2 \mod 7, & 5^5 \equiv 3 \mod 7.
\end{array}
$$

$$
\begin{array}{lll}
3^0 \equiv 1 \mod 7, & 3^1 \equiv 3 \mod 7, & 3^2 \equiv 2 \mod 7, \\
3^3 \equiv 6 \mod 7, & 3^4 \equiv 4 \mod 7, & 3^5 \equiv 5 \mod 7.
\end{array}
$$

Por tanto, podemos calcular logaritmos en base 5 y base 3. Ej:

$$
\begin{array}{l}
5^3 \equiv 6 \mod 7 \Rightarrow \log_5 6 = 3 \mod 7, \\
3^3 \equiv 6 \mod 7 \Rightarrow \log_3 6 = 3 \mod 7.
\end{array}
$$

<u>Problema</u>: Cómo obtener los generadores de $\mathbb{Z}_p^*$.

Subgrupo

Dado un grupo, se denomina *subgrupo* a un subconjunto que posee estructura de grupo para la operación del grupo.

- El orden de un subgrupo divide al orden del grupo.

Ejemplo

$\mathbb{Z}_7^* = \{1, 2, 3, 4, 5, 6\}$

Observemos que 2, 4 y 6 no son generadores:

$$\begin{array}{llll} 2^0 \equiv 1 \mod 7, & 2^1 \equiv 2 \mod 7, & 2^2 \equiv 4 \mod 7, & 2^3 \equiv 1 \mod 7, \\ 4^0 \equiv 1 \mod 7, & 4^1 \equiv 4 \mod 7, & 4^2 \equiv 2 \mod 7, & 4^3 \equiv 1 \mod 7, \\ 6^0 \equiv 1 \mod 7, & 6^1 \equiv 6 \mod 7, & 6^2 \equiv 1 \mod 7, & \end{array}$$

*	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

$$\{1, 2, 4\} \subset \mathbb{Z}_7^*,\ \{1, 6\} \subset \mathbb{Z}_7^*,\ \textit{son subgrupos, y son cíclicos}.$$

Teorema

- *Todo subgrupo de un grupo cíclico es cíclico.*
- *Un grupo cíclico posee un único subgrupo de orden cada divisor del orden del grupo.*
- *Un grupo cíclico de orden m tiene $\phi(m)$ generadores.*

Ejemplo

$\mathbb{Z}_7^* = \{1, 2, 3, 4, 5, 6\}$. $(\mathbb{Z}_7^*, \cdot)$ es un grupo cíclico de orden 6

- Los divisores de 6 son 1, 2, 3 y 6
- Existe un único subgrupo para cada orden 1, 2, 3 y 6:
$$\{1\}, \quad \{1, 6\}, \quad \{1, 2, 4\}, \quad \mathbb{Z}_7^*$$
- Los subgrupos son cíclicos, y poseen, respectivamente,
$$\phi(1) = 1, \quad \phi(2) = 1, \quad \phi(3) = 2, \quad \phi(6) = 2 \ \ \textit{generadores}$$

Subgrupo generado por a

Dado un elemento $a \in Z_p^*$, se llama *orden* de a, ord(a), al mínimo entero positivo t tal que

$$a^t \equiv 1 \mod p$$

Ejemplo

$\mathbb{Z}_7^* = \{1, 2, 3, 4, 5, 6\}$

$$2^0 \equiv 1 \mod 7, \quad 2^1 \equiv 2 \mod 7, \quad 2^2 \equiv 4 \mod 7, \quad 2^3 \equiv 1 \mod 7,$$

$$\Rightarrow \mathrm{ord}(2) = 3$$

Se tiene que:

- Dado $a \in Z_p^*$

$$a \text{ es generador de } Z_p^* \Leftrightarrow ord(a) = p - 1.$$

- Dado $a \in Z_p^*$ de orden t,

$$\{a^k \mod p, \; k = 1, 2, \ldots, t\}$$

es el subgrupo generado por a de orden t.

Ejemplo

$$\mathbb{Z}_{11}^* = \{1,2,3,4,5,6,7,8,9,10\}$$

- El orden de $(\mathbb{Z}_{11}^*, \cdot)$ es 10
- Los divisores de 10 son 1, 2, 5 y 10
- Existe un único subgrupo para cada orden 1, 2, 5 y 10:
  (cualquier elemento de $\mathbb{Z}_{11}^*$ tiene orden $1, 2, 5$ o 10)

$$\begin{array}{llll}
2^2 \equiv 4 \mod 11, & 2^5 \equiv 10 \mod 11 & \Rightarrow & \mathrm{ord}(2) = 10 \\
3^2 \equiv 9 \mod 11, & 3^5 \equiv 1 \mod 11 & \Rightarrow & \mathrm{ord}(3) = 5 \\
10^2 \equiv 1 \mod 11, & & \Rightarrow & \mathrm{ord}(10) = 2
\end{array}$$

2 es generador de $\mathbb{Z}_{11}^*$
3, 10 no son generadores de $\mathbb{Z}_{11}^*$

$2, 6, 7, 8$ son generadores de $\mathbb{Z}_{11}^*$, $\quad \phi(10) = 4$
$3, 4, 5, 9$ son generadores de $\{1, 3, 4, 5, 9\}$, $\quad \phi(5) = 4$
10 es generador de $\{1, 10\}$, $\quad \phi(2) = 1$

Intercambio de claves de Diffie-Hellman

En 1976 W. Diffie y M. E. Hellman diseñaron un método para intercambiar claves secretas en un canal abierto.

Este método fue el origen de la criptografía de *clave pública*.

Se fundamenta en el *problema de Diffie-Hellman*, basado en el *problema del cálculo de logaritmo discreto*.

Problema de Diffie-Hellman:

Dado un número primo p, un número g que sea generador de $\mathbb{Z}_p^*$ y los números g^a y g^b, encontrar g^{ab} (mod p).

Se conoce g^a, g^b, pero no se conoce a, b.

Resolviendo el problema del cálculo de logaritmo discreto, se resuelve el problema de Diffie-Hellman.

Intercambio de claves de Diffie-Hellman

Objetivo: A y B pretenden intercambiar una clave secreta a través de un canal abierto.

A y B acuerdan un número primo grande p y un generador g de $\mathbb{Z}_p^*$. La información (p, g) es **pública**.

Protocolo:

- A elige un número aleatorio x_A , $0 < x_A < p-1$ y envía
$$g^{x_A} \mod p.$$
- B elige un número aleatorio x_B , $0 < x_B < p-1$ y envía
$$g^{x_B} \mod p.$$
- B recoge $g^{x_A} \mod p$ y calcula: $K \equiv (g^{x_A})^{x_B} \equiv g^{x_A x_B} \mod p$.
- A recoge $g^{x_B} \mod p$ y calcula: $K \equiv (g^{x_B})^{x_A} \equiv g^{x_B x_A} \mod p$.

La clave secreta intercambiada es K.

Ejemplo

A y B pretenden intercambiar una clave secreta para su utilización en un algoritmo simétrico.
Acuerdan un primo $p = 71$ y un generador $g = 21$ del grupo $\mathbb{Z}_{71}^*$.

- A elige un número secreto $x_A = 46$ y envía
$$21^{46} \equiv 9 \mod 71.$$
- B elige un número secreto $x_B = 57$ y envía
$$21^{57} \equiv 61 \mod 71.$$
- B calcula $K \equiv 9^{57} \equiv 16 \mod 71$.
- A calcula $K \equiv 61^{46} \equiv 16 \mod 71$.

La clave intercambiada es $K \equiv 16 \mod 71$.

Ataque a Diffie-Hellman

Man-in-the-middle:

A		C		B
$1 < x_A < p-1$		$1 < x_C < p-1$		$1 < x_B < p-1$
	$\rightarrow$		$\rightarrow$	
	$y_A = g^{x_A}$		$y_C = g^{x_C}$	
	$\leftarrow$		$\leftarrow$	
	$y_C = g^{x_C}$		$y_B = g^{x_B}$	
	$z_{AC} = g^{x_A x_C}$		$z_{CB} = g^{x_B x_C}$	

Nota: Todas las potencias son modulares, módulo p

Para evitarlo:

- Control de tiempo
- Autenticación de origen

Criptosistema ElGamal

El sistema de cifrado de ElGamal (1985) es un sistema de clave pública basado en la dificultad del cálculo del logaritmo discreto.

Generación de claves en ElGamal

Cada entidad:

- Obtiene un p, número primo grande.
- Halla g, generador de $\mathbb{Z}_p^*$.
- Elige: x, número aleatorio, $1 < x < p - 1$.
- Calcula: $y \equiv g^x \mod p$.

Clave *pública del receptor:* (p, g, y).
Clave *privada del receptor:* x.

Cifrado y descifrado en ElGamal

Sea un mensaje M, $M \in \mathbb{Z}_p$.
Sea (p, g, y) la clave pública del receptor, y x su clave privada.

- Función de cifrado: El emisor elige un número secreto b, $1 < b < p - 1$.

$$\begin{array}{ccc} \mathbb{Z}_p & \xrightarrow{\mathrm{E}} & \mathbb{Z}_p \times \mathbb{Z}_p \\ M & \mapsto & C = (r, s) \end{array}$$

  donde
$$r \equiv g^b \mod p, \quad s \equiv My^b \mod p.$$

- Función de descifrado

$$\begin{array}{ccc} \mathbb{Z}_p \times \mathbb{Z}_p & \xrightarrow{\mathrm{D}} & \mathbb{Z}_p \\ C = (r, s) & \mapsto & s(r^x)^{-1} \mod p. \end{array}$$

<u>Observaciones</u>:

Mensajes idénticos originan cifrados diferentes

Desventaja: longitud del mensaje cifrado doble

$$C = (r, s) \text{ donde } r \equiv g^b \pmod{p}, \quad s \equiv My^b \pmod{p}.$$

$$\mathrm{D}(r, s) \equiv s(r^x)^{-1} \pmod{p}.$$

Justificación:

$$\mathrm{D}(\mathrm{E}(M)) \stackrel{?}{=} M$$

$$\mathrm{D}(\mathrm{E}(M)) = \mathrm{D}(r, s) \equiv s(r^x)^{-1} \equiv My^b((g^b)^x)^{-1}$$
$$\equiv M(g^x)^b(g^{bx})^{-1} \equiv Mg^{xb}(g^{bx})^{-1} \equiv M \pmod{p}.$$

Observación:

- $r^x r^{p-1-x} \equiv r^{p-1} \equiv 1 \pmod{p} \Rightarrow (r^x)^{-1} \equiv r^{p-1-x} \pmod{p}$. Por tanto,

$$\mathrm{D}(r, s) \equiv s(r^x)^{-1} \equiv sr^{p-1-x} \pmod{p}.$$

Ejemplo

A quiere enviar a B el mensaje $M = 5$ cifrado.
$(p, g, y) = (71, 21, 17)$ clave pública de un criptosistema ElGamal de B.
La clave secreta de B es $x = 7$ $(y \equiv 21^7 \mod 71 \equiv 17)$.

- A elige un número b, $1 < b < 70$. Por ejemplo $b = 3$.
- Calcula
  - $r \equiv 21^3 \equiv 31 \mod 71$,
  - $s \equiv 5 \cdot 17^3 \equiv 70 \mod 71$.
- A envía $C = (r, s) = (31, 70)$.
- El receptor B recibe $C = (r, s) = (31, 70)$.

  Calcula
  $$sr^{p-1-x} \equiv 70 \cdot 31^{70-7} \equiv 5 \mod 71.$$
  y obtiene el mensaje $M = 5$.

Fin de la sección