Problema de Diffie-Hellman

Suponha-se que um adversário pretende recuperar m a partir do conhecimento da chave pública (p, g, r) e do texto cifrado (γ, δ).

De $m \equiv \gamma^{p-1-a}\delta \pmod p$ e $\gamma \equiv g^k \pmod p$ resulta que $m \equiv g^{k(p-1)-ka}\delta \pmod p$ e, portanto, $g^{ka}m \equiv g^{k(p-1)}\delta \equiv \delta \pmod p$.

Se o adversário conseguir determinar o resto da divisão de g^{ka} por p, o que corresponde a resolver o problema de Diffie-Hellman, só tem que resolver uma congruência linear para recuperar m.

Definição (Problema de Diffie-Hellman)

Dados p primo, g uma raíz primitiva módulo p e os restos da divisão de g^a e g^k por p (onde $a, k \in \mathbb{N}$ não são conhecidos) determinar o resto da divisão de g^{ak} por p.

Problema do Logaritmo Discreto

Suponha-se que um adversário pretende obter a chave privada do receptor, a, a partir do conhecimento da chave pública (p, g, r).

Como determinar $a \in \{1, 2, \ldots, p-2\}$ tal que $g^a \equiv r \pmod p$?

Isto corresponde a resolver o problema do logaritmo discreto.

Definição (Logaritmo Discreto em $\mathbb{Z}_p^*$)

Considere-se p primo e g raíz primitiva módulo p.
Dado $b \in \mathbb{Z}$ tal que $p \nmid b$ existe um único $t \in \{0, 1, 2, \ldots, p-2\}$ tal que $g^t \equiv b \pmod p$.
O t, nestas condições, é o logaritmo discreto de b na base g (módulo p) e representa-se por $\log_g b$.

Propriedades do Logaritmo Discreto

Sejam g e g' duas raízes primitivas módulo p, $k \in \mathbb{N}$ e $a, b \in \mathbb{Z}$ primos com p. Então:

- $a \equiv b \pmod p \rightarrow \log_g a = \log_g b$;
- $\log_g(ab) \equiv \log_g a + \log_g b \pmod{p-1}$;
- $\log_g(a^k) \equiv k \log_g a \pmod{p-1}$;
- $\log_g g' \log_{g'} a \equiv \log_g a \pmod{p-1}$.

Demonstração

Demonstração: Sejam $l = \log_g a$ e $t = \log_g b$.

Se $a \equiv b \pmod p$ então $g^l \equiv g^t \pmod p$ e $g^{|t-l|} \equiv 1 \pmod p$. Então $|t-l|$ é um múltiplo de $\mathrm{ord}_p g = p-1$, concluindo-se, porque $0 \leq t, l \leq p-2$, que $l = t$.

Seja $r = \log_g(ab)$. De $g^r \equiv ab \equiv g^l g^t \equiv g^{l+t} \pmod p$ resulta que $g^{|l+t-r|} \equiv 1 \pmod p$ e, portanto, $l + t - r$ é um múltiplo de $p-1$.

Seja $s = \log_g(a^k)$. De $g^s \equiv a^k \equiv (g^l)^k \equiv g^{lk} \pmod p$ resulta que $g^{|lk-s|} \equiv 1 \pmod p$ e, portanto, $lk - s$ é um múltiplo de $p-1$.

Sejam $u = \log_g g'$ e $v = \log_{g'} a$. De $g^{|uv-l|} \equiv a \equiv (g')^v \equiv g^{uv} \pmod p$, resulta que $g^{|uv-l|} \equiv 1 \pmod p$ e, portanto, $uv - l$ é um múltiplo de $p-1$.

□

Problema do Logaritmo Discreto

Definição (Problema do Logaritmo Discreto)

Dados p primo, g uma raíz primitiva módulo p e $b \in \mathbb{Z}$ tal que $p \nmid b$, determinar o logaritmo discreto de b na base g.

A dificuldade de resolução do problema do logaritmo discreto não depende da raíz primitiva que se considera, porque, sendo g e g' duas raízes primitivas módulo p, tem-se $\log_g g' \log_{g'} b \equiv \log_g b (\mathrm{mod}\ p-1)$.

Logaritmo Discreto/Diffie-Hellman

Definição (Problema Diffie-Hellman)

Dados p primo, g uma raíz primitiva módulo p e os restos da divisão de g^a e g^b por p (onde $a, b \in \mathbb{N}$ não são conhecidos) determinar o resto da divisão de g^{ab} por p.

Se for conhecida a resolução do problema do logaritmo discreto é possível resolver o problema de Diffie-Hellman:

Calcula-se $t = \log_g(g^b)$;

$t \equiv b (\mathrm{mod}\ p-1)$, logo, $g^{ab} \equiv (g^a)^t (\mathrm{mod}\ p)$.

Algoritmo de Shanks

Proposição (Algoritmo de Shanks)

Sejam p um número primo, g uma raíz primitiva módulo $p, a, b \in \{1, \ldots, p-1\}$ e $m = \lceil \sqrt{p-1} \rceil$.

Se $g^m a \equiv 1 (\mathrm{mod}\ p)$ então existem

$i, j \in \{0, 1, \ldots, m-1\}$ *tais que* $a^i b \equiv g^j (\mathrm{mod}\ p)$.

Mais, para i e j nestas condições,

$$log_g b \equiv im + j (\mathrm{mod}\ p-1).$$

Demonstração

Seja $k = \log_g b$. Isto é, $k \in \{0, 1, \ldots, p-2\}$ e $g^k \equiv b (\mathrm{mod}\ p)$.

Se $k \leq m - 1 = \lceil \sqrt{p-1} \rceil - 1$ basta considerar $i = 0$ e $j = k$. Se $k \geq m$ então $k = im + j$ com $1 \leq i \leq m-1$ e $0 \leq j \leq m-1$.

$$\begin{aligned} b \equiv g^{im+j} (\mathrm{mod}\ p) &\Rightarrow a^i b \equiv a^i g^{im} g^j (\mathrm{mod}\ p) \\ &\Rightarrow a^i b \equiv (ag^m)^i g^j (\mathrm{mod}\ p) \\ &\Rightarrow a^i b \equiv g^j (\mathrm{mod}\ p). \end{aligned}$$

Além disso, se i, j são tais que $a^i b \equiv g^j (\mathrm{mod}\ p)$ então

$$\begin{aligned} a^i g^{im+j} = (ag^m)^i g^j &\Rightarrow a^i g^{im+j} \equiv g^j (\mathrm{mod}\ p) \\ &\Rightarrow a^i g^{im+j} \equiv a^i b (\mathrm{mod}\ p) \\ &\Rightarrow g^{im+j} \equiv b (\mathrm{mod}\ p) \\ &\Rightarrow im + j \equiv \log_g b (\mathrm{mod}\ p-1). \end{aligned}$$

Observação:
Uma vez que $\mathrm{mdc}(p, g^m) = 1$, g^m é invertível em $\mathbb{Z}_p^*$ e, portanto, existe $a \in \{1, \ldots, p-1\}$ tal que $g^m a \equiv 1 (\mathrm{mod}\ p)$.

Algoritmo de Shanks

Entrada: p primo, g raíz primitiva módulo p e um inteiro b primo com p

Saida: $\log_g b$

$m \leftarrow \lceil \sqrt{p-1} \rceil$
Constrói-se uma tabela $(j, g^j \bmod p)$, $j = 0, 1, \ldots, m-1$
Determina-se $a \in \{1, \ldots, p-1\}$ tal que $g^m a \equiv 1 (\bmod\ p)$
$c \leftarrow b$;
$i \leftarrow 0$;
`enquanto` c não aparece na segunda linha da tabela `faz`
    $c \leftarrow ca$;
    $i \leftarrow i + 1$;
`fimenquanto`
Se $c \equiv g^j (\bmod\ p)$, a saída é o resto da divisão de $im + j$ por $p - 1$.

Exemplo

$p = 157; g = 5$ é uma raíz primitiva módulo 157.
$\log_5 18 = ?$
$m \leftarrow \lceil \sqrt{156} \rceil = 13$

Constrói-se a tabela

j	0	1	2	3	4	5	6	7	8	9	10	11	12
$5^j \bmod 157$	1	5	25	125	154	142	82	96	9	45	68	26	130

Ordena-se a tabela pela segunda linha:

j	0	1	8	2	11	9	10	6	7	3	12	5	4
$5^j \bmod 157$	1	5	9	25	26	45	68	82	96	125	130	142	154

Determina-se $1 \leq a \leq 156$ tal que $5^{13} a \equiv 1 (\bmod\ 157) : a = 50$

Exemplo

Começando com $i = 0$ procura-se o primeiro i tal que $50^i 18$ é congruente com 5^j, para $0 \leq j \leq 12$:

i	0	1	2	3	4	5	6	7	8	9	10	11
$50^i 18 \bmod 157$	18	115	98	33	80	75	139	42	59	124	77	82

Para $i = 11$ e $j = 6$ tem-se $50^i 18 \equiv 5^j (\bmod\ 157)$

$\log_5 18$ é o resto da divisão de $im + j = 11 \times 13 + 6 = 149$ por 156.

$\log_5 18 = 149$, isto é, $5^{149} \equiv 18 (\bmod\ 157)$

Bibliografia I

D. Atkins, M. Graff, A. Lenstra, and P. Leyland.
The magic words are squeamish ossifrage.
In *ASIACRYPT 1994*, pages 263–277, 1994.

Eli Biham and Adi Shamir.
Differential cryptanalysis of DES-like cryptosystems.
Journal of Cryptology, 4(1):3–72, jan 1991.
doi: 10.1007/BF00630563.

Grady Booch.
Object Oriented Analysis and Design, with Applications.
Addison Wesley Longman, Inc., 2nd edition, 1994.
DMAT 68N/BOO; Programação Orientada para objectos.

Johannes Buchmann.
Introduction to Cryptography.
Springer-Verlag, New York, 2000.